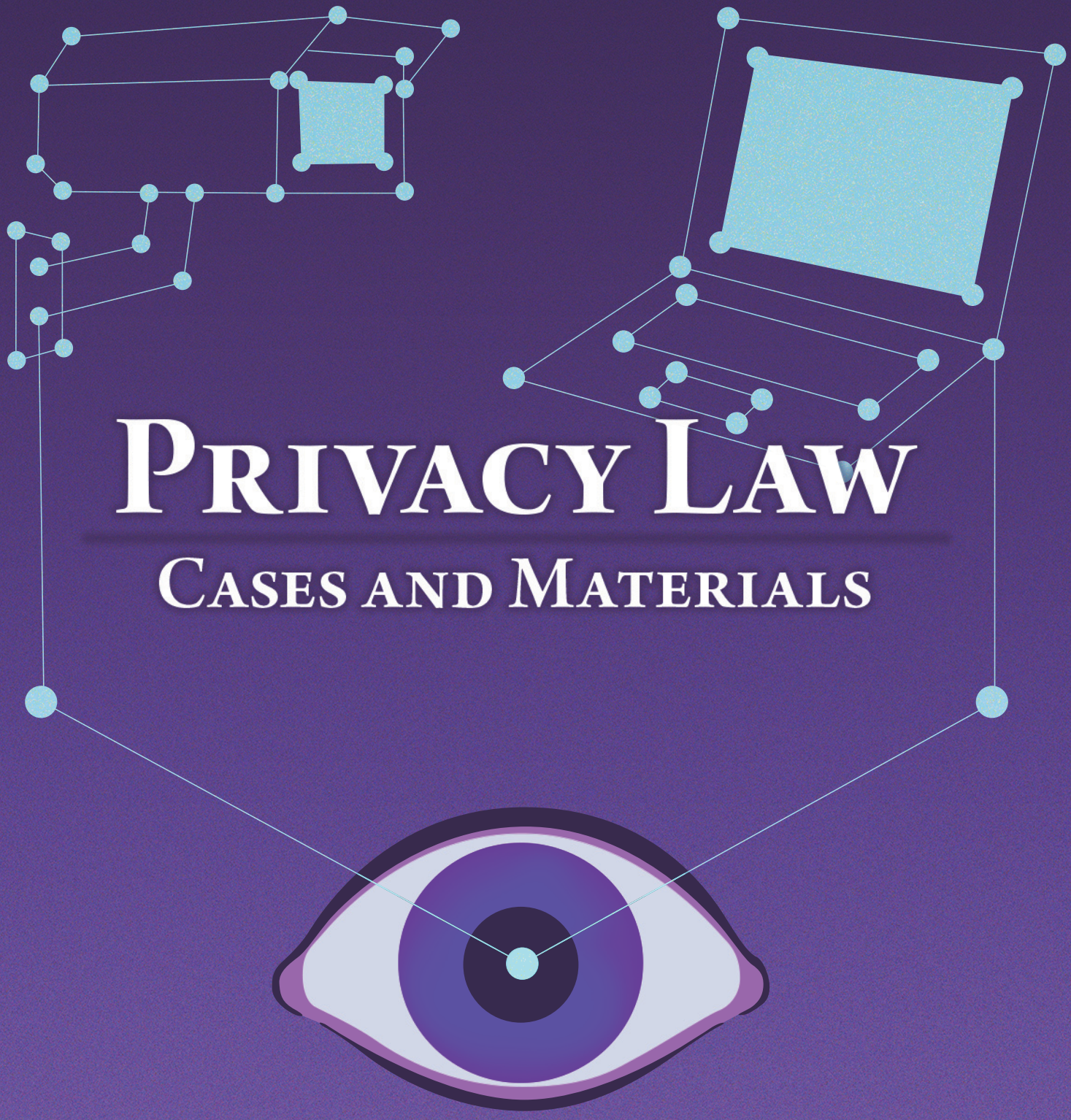


Privacy Law

Cases and Materials

3rd Edition, 2026

Matthew B. Kugler

Privacy Law: Cases and Materials

3rd Edition 2026

privacycasebook.com

Matthew B. Kugler

Professor of Law

Northwestern Pritzker School of Law

For generous comments on earlier versions of this casebook, I am grateful to Anne Boustead, Aileen Neilsen, Przemysław Pałka, and Charlotte Tschider. Thanks also to Perry Asibey-Bonsu. Justin Lai, Edward Lee, Alena Prcela, and Samuel Pritchard for extraordinary research assistance.

© 2026, Matthew B. Kugler

Excerpts from cases, statutes, and other government works are in the public domain. Other excerpted materials are used with permission or under the fair use provisions of 17 U.S.C. § 107.

The cover art was created by Myriam Bloom, https://myriambloom.com/

Electronic versions of this book can be freely distributed provided that the document retains its cover page and continues to attribute authorship to me. Physical copies may be printed for personal use, but commercial print distribution should only be through channels I have previously authorized. I am likely willing to authorize many derivative uses—please contact me if you have any ideas you would like to discuss (matthew.kugler@law.northwestern.edu).

When editing cases and other materials, the goal has been pedagogical clarity, not *Bluebook*-compliant accuracy. Citations and portions of text have been omitted without the usual ellipses and brackets where they seemed more cumbersome than helpful.

I could have made the cases shorter, but the Supreme Court couldn't.
It is really all their fault.

For my parents, who have never fully understood
my career but always encouraged me anyway.

I. PRIVACY FUNDAMENTALS 1

A. In the beginning 1
Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) 2

B. Privacy values – What is privacy and why is it important? 9
1) Privacy's individual function 9
Alan Westin, Privacy and Freedom (1967) 10
2) Privacy's societal function 12
Julie E. Cohen, *Examined Lives*, 52 STAN. L. REV. 1373 (2000) 12
Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723 (1999) 15

C. Privacy costs – Is privacy good? 17
Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978) 17

D. Feminist critique 21
Michela Meister and Karen Levy, Digital Security and Reproductive Rights: Lessons for Feminist Cyberlaw (2024) 21

II. TORT PRIVACY AND INDIVIDUAL PRIVACY ACTIONS 24

A. Intrusion upon seclusion 25
Howard v. Aspen Way Enterprises, Inc., 406 P.3d 1271 (Wyo. 2017) 25
Safari Club International v. Rudolph, 862 F.3d 1113 (9th Cir. 2017) 28
Desnick v. American Broadcasting Companies, Inc., 44 F.3d 1345 (7th Cir. 1995) 33
Council on American-Islamic Relations Action Network, Inc. v. Gaubatz, 793 F.Supp.2d 311 (D.D.C. 2011) 36

B. Public disclosure of private facts 40
1) Elements of public disclosure 40
Finley v. Kelly, 384 F.Supp.3d 898 (M.D. Tenn. 2019) 40
In re Facebook, Inc., Consumer Privacy User Profile Litig., 402 F.Supp.3d 767 (N.D. Cal. 2019) 43
2) Newsworthiness 50
Shulman v. Group W Productions, Inc., 955 P.2d 469 (Cal. 1998) 50
Y.G. v. Jewish Hospital of St. Louis, 795 S.W.2d 488 (Mo. App. 1990) 57
3) Republisher Immunity 63
Sipple v. Chronicle Publishing Co., 154 Cal.App.3d 1040 (1984) 63
4) First Amendment Limitations on Public Disclosure Liability 67
Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975) 68
The Florida Star v. B.J.F., 491 U.S. 524 (1989) 71
Publius v. Boyer–Vine, 237 F.Supp.3d 997 (E.D. Cal. 2017) 79
Bartnicki v. Vopper, 532 U.S. 514 (2001) 83
Boehner v. McDermott, 484 F.3d 573 (D.C. Cir. 2007) 90

C. False Light and Defamation 95
1) False light 95
2) Defamation 95
Eramo v. Rolling Stone, LLC, 209 F.Supp.3d 862 (W.D. Va. 2016) 96
3) Section 230 as a bar to liability 101
Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997) 102

D. Right of Publicity 107
White v. Samsung Electronics America, Inc. 971 F.2d 1395 (9th Cir. 1992) 109
Young v. NeoCortext, Inc., 690 F. Supp. 3d 1091 (C.D. Cal. 2023) 113

E. Nonconsensual pornography and image-based sexual abuse 119
State v. VanBuren, 214 A.3d 791 (Vt. 2019) 119
15 U.S. Code § 6851 - Civil action relating to disclosure of intimate images 128
The Take It Down Act 132

III. GOVERNMENT INVESTIGATIONS 134

A. Fourth Amendment and law enforcement searches 135
1) The *Katz* Test 136
Katz v. United States, 389 U.S. 347 (1967) 137
United States v. White, 401 U.S. 745 (1971) 140
2) The Third-Party Doctrine 143
Smith v. Maryland, 442 U.S. 735 (1979) 143

B. Constitutional limitations and new technologies 148
1) Changing surveillance and communication technologies 149
Kyllo v. United States, 533 U.S. 27 (2001) 149
United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) 152
2) Location Tracking 156
United States v. Jones, 565 U.S. 400 (2012) 156
Carpenter v. United States, 585 U.S. 296 (2018) 163
Chatrie v. United States, 609 U.S. ___ (2026) 172
3) Digital Searches 185
Riley v. California, 573 U.S. 373 (2014) 186

C. Constitutional limitations on non-law enforcement searches 193
Vernonia School Dist. 47J v. Acton, 515 U.S. 646 (1995) 194
Ferguson v. City of Charleston, 532 U.S. 67 (2001) 200

D. Wiretapping and the Electronic Communications Privacy Act 206
1) The Wiretap Act 207
a) Interception by the government 209
b) Interception by private actors and penalties 210
c) Exclusionary rule 210
2) State Wiretap Law 211
3) The Pen Register Act 212
4) The Stored Communications Act 213
a) Required disclosures under 18 U.S.C § 2703 214
b) Limits on voluntary disclosure under 18 U.S.C § 2702 215
c) Penalties 215

IV. NATIONAL SECURITY 217

A. Overall framework 217
U.S. v. U.S. Dist. Court for Eastern Dist. of Mich., 407 U.S. 297 (1972) [The Keith Case] 218

B. Foreign Intelligence Surveillance Act 224
In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) 225
United States v. Aziz, 228 F.Supp.3d 363 (M.D. Penn. 2017) 235

C. National Security Letters 237
1) Types of National Security Letters 238
2) Constitutionality of Gag Orders 240

D. Section 215 and the metadata program 240
United States v. Moalin 973 F.3d 977 (9th Cir. 2020) 241

E. Section 702 and surveillance overseas 248
Clapper v. Amnesty Intern. USA, 568 U.S. 398 (2013) 249
United States v. Muhtorov, 20 F.4th 558 (10th Cir. 2021) 257

V. SUBSTANTIVE DUE PROCESS 267

A. The beginnings of constitutional decision privacy 267
1) *Griswold*, history, and the start of the journey 268
Griswold v. Connecticut, 381 U.S. 479 (1965) 268
2) Abortion prior to *Dobbs* 271
3) Life, death, and gay rights 272
Washington v. Glucksberg, 521 U.S. 702 (1997) 272
Lawrence v. Texas, 539 U.S. 558 (2003) 276

B. Dobbs and the future of the right to decision privacy 280
Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022) 280

C. The right to information privacy 287
1) Foundations 287
Whalen v. Roe, 429 U.S. 589 (1977) 287
National Aeronautics and Space Administration v. Nelson, 562 U.S. 134 (2011) 292
2) Circuit level reactions to uncertainty 299
Dillard v. O'Kelley, 961 F.3d 1048 (8th Cir. 2020) 299
Sterling v. Borough of Minersville, 232 F.3d 190 (3rd Cir. 2000) 305

VI. GOVERNMENT RECORDS 309

A. Freedom of Information Act 309
U.S. Dept. of Justice v. Reporters Committee for Freedom of Press, 489 U.S. 749 (1989) 311
National Archives and Records Administration v. Favish, 541 U.S. 157 (2004) 317

B. Fair Information Practices and the Privacy Act 322
Dinh Tran v. Department of Treasury, 351 F.Supp.3d 130 (D.D.C. 2019) 325
Doe v. Chao, 540 U.S. 614 (2004) 328
F.A.A. v. Cooper, 566 U.S. 284 (2012) 333
In re U.S. OPM Data Security Breach Litig., 928 F.3d 42 (D.C. Cir. 2019) 338

VII. HEALTH PRIVACY 343

A. Common law roots of medical privacy 343
1) Duty of Confidentiality 344
Lawson v. Halpern-Reiss, 212 A.3d 1213 (2019) 344
2) Evidentiary Privileges 348
Jaffee v. Redmond, 518 U.S. 1 (1996) 348
3) Duty to Warn 354

Tarasoff v. Regents of University of California, 551 P.2d 334 (Cal. 1976) 354

B. The rise of HIPAA 359
1) The Privacy, Security, and Data Breach Rules 360
a) Limitations on the use and disclosure of PHI under the Privacy Rule 361
b) Data security requirements under the Security Rule 364
c) Data breach notification 365
2) State Medical Privacy Law as a Supplement to HIPAA 366
Shepherd v. Costco Wholesale Corporation, 482 P.3d 390 (Ariz. 2021) 368
3) HIPAA Civil Enforcement 371
Premera Blue Cross Resolution Agreement (2020) 373
Athens Orthopedic Clinic Resolution Agreement (2020) 375
Yakima Valley Memorial Hospital Press Release (2023) 377
4) HIPAA Criminal Enforcement 379
U.S. v. Huping Zhou, 678 F.3d 1110 (2012) 379

C. Privacy in genetic information 382
1) Use of genetic information for identification 382
Maryland v. King, 569 U.S. 435 (2013) 382
2) Use of genetic information for prediction 390

VIII. FINANCIAL PRIVACY 393

A. The Common Law 393
Dwyer v. American Express Company, 652 N.E.2d 1351 (Ill App. Ct.1995) 393

B. Gramm–Leach–Bliley Act 397

C. Fair Credit Reporting Act 400
1) Scope of the Act 400
2) Protections under the FCRA 401
United States v. Spokeo, Inc., CV12-05001 (C.D. Cal. 2012) 403
Erickson v. First Advantage Background Services Corp., 981 F.3d 1246 (11th Cir. 2020) 406
3) Federal Standing and FCRA claims 410
TransUnion LLC v. Ramirez, 594 U.S. 413 (2021) 412

IX. CONSUMER PRIVACY 424

A. Federal Trade Commission and Section 5 425
United States v. Easy Healthcare Corp., Case No. 1:23-cv-3107 (N.D. Ill. 2023) 426
United States v. Facebook, Inc. Case No. 19-cv-2184 (D.C. Dist. Ct. 2019) 432
In the Matter of Support King, LLC (SpyFone.com) (FTC 2021) 439
FTC v. Rite Aid Corp., No. 2:23-cv-5023 (E.D. Penn. 2023) 442
In the Matter of X-Mode Social, Inc. and Outlogic, LLC, C-4802 (FTC 2024) 448

B. Children's Privacy 456
1) Children's Online Privacy Protection Act 456
F.T.C. and N.Y. v. Google LLC and YouTube, LLC (D.D.C. 2019) 459
United States v. Epic Games, Inc. (E.D.N.C. 2022) 466
2) California Age-Appropriate Design Code Act 473
NetChoice, LLC v. Bonta, 170 F.4th 744 (9th Cir. 2026) 474

C. Marketing Privacy 485
1) CAN-SPAM Act 485

2) Telephone Consumer Protection Act 487

D. Tracking Privacy 487
1) ECPA and Online Tracking 487
In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589 (9th Cir. 2020) 487
2) Video Privacy Protection Act 495
In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 (3rd Cir. 2016) 495
Gardner v. Me-TV National Limited Partnership, 132 F.4th 1022 (7th Cir. 2025) 504

E. Biometric Privacy 506
Rosenbach v. Six Flags Entertainment Corporation, 129 N.E.3d 1197 (Ill. 2019) 508
Patel v. Facebook 932 F.3d 1264 (9th Cir. 2019) 513
Zellmer v. Meta, 104 F.4th 1117 (9th Cir. 2024) 519
Cothron v. White Castle System, Inc., 216 N.E.3d 918 (Ill. 2023) 525

F. Comprehensive State Privacy Laws 528
1) California Consumer Privacy Act 528
California v. Sephora USA, Inc. (Cal. Super. Ct. 2022) 533
American Honda Motor Co., No. ENF23-V-HO-2 (Cal. Privacy Prot. Agency, 2025) 537
California Delete Act 545
2) Other states 546

X. DATA SECURITY 551

A. Data Breach Notification Laws 551

B. Data Breach Lawsuits 554
Tsao v. Captiva MVP Restaurant Partners, LLC, 986 F.3d 1332 (11th Cir. 2021) 554
In re Equifax, Inc., Customer Data Security Breach Litig., 362 F.Supp.3d 1295 (N.D. Ga. 2019) 562

C. Federal Trade Commission and Data Security 571
FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015) 573
LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018) 579
In the Matter of Chegg, Inc. (FTC 2023) 585

XI. WORKPLACE PRIVACY 589

A. Government Employees 590
O'Connor v. Ortega, 480 U.S. 709 (1987) 590

B. Employees and the privacy torts 599
Clark v. Teamsters Local Union 651, 349 F.Supp.3d 605 (E.D. Ky. 2018) 599
Horgan v. Simmons, 704 F.Supp.2d 814 (N.D. Ill. 2010) 601

C. Laws on specific subjects 604
1) Employees and the Electronic Communications Privacy Act (ECPA) 604
Owen v. Cigna, 188 F.Supp.3d 790 (N.D. Ill. 2016) 604
Sullinger v. Sullinger, 849 Fed.Appx. 513 (6th Cir. 2021) (unpublished) 606
Democracy Partners v. Project Veritas Action Fund, 285 F.Supp.3d 109 (D.D.C. 2018) 608
2) Cameras in the workplace 611
3) GPS monitoring of vehicles 612
Cunningham v. New York State Department of Labor, 997 N.E.2d 468 (N.Y. 2013) 613
4) Drug testing 616

XII. EUROPEAN PRIVACY LAW 618

A. The European Convention on Human Rights 619
Von Hannover v. Germany, No. 59320/00, Eur. Ct. H.R 294 (2004) 621

B. The Data Protection Directive and the Right to be Forgotten 630
Google Spain SL v. Agencia Española de Protección de Datos (AEPD), No. C-131/12, E.C.J. (2014) 630

C. Basic Features of the General Data Protection Regulation 639
Bundesverband der Verbraucherzentralen und Verbraucherverbände v. Planet49 GmbH, No. C-673/17, E.C.J. (2019) 643
Meta v Bundeskartellamt, No. C-252/21, E.C.J. (2023) 649

D. GDPR and International Data Transfers 657
Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximilian Schrems (*Schrems II*), No. C-311/18, E.C.J. (2020) 658

I. Privacy Fundamentals

A. In the beginning 1
Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) 2

B. Privacy values – What is privacy and why is it important? 9
1) Privacy's individual function 9
Alan Westin, Privacy and Freedom (1967) 10
2) Privacy's societal function 12
Julie E. Cohen, *Examined Lives*, 52 STAN. L. REV. 1373 (2000) 12
Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723 (1999) 15

C. Privacy costs – Is privacy good? 17
Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978) 17

D. Feminist critique 21
Michela Meister and Karen Levy, Digital Security and Reproductive Rights: Lessons for Feminist Cyberlaw (2024) 21

A. In the beginning

You are being watched.

The shape and nature of privacy has changed drastically over the past fifty years. Where once a person could move to a new town and adopt a new life, leaving behind all that came before, now pictures and data can follow even the most obscure individual for decades. A person taking a short walk down the street will pass dozens of cameras. Some of these cameras will be controlled by private individuals concerned about the theft of their delivery orders, some by government agencies concerned with traffic enforcement, and some, perhaps, by actors who may wish them ill. What protections do people have against this new world of perpetual surveillance? As we shall see, very little in many cases.

Unlike some other areas of law with roots tracing back centuries, if not millennia, privacy law is a relatively recent innovation. And, from its beginning, the story of privacy law has been one of technological change. As new technologies are invented, they raise new concerns. In 1890, two writers posited the existence of a "Right to Privacy" in an article in the *Harvard Law Review*. This piece has sometimes been called the most influential law review article in American history. Though one might fairly question the stiffness of the competition for that title, the piece is still impressively influential.

The authors of the article are Louis Brandeis, later a prominent Supreme Court Justice, and Samuel Warren, a highly successful attorney. Their exact motivations for writing the piece are unclear, but both were exactly the sort of "society" gentlemen whose comings and goings would regularly attract the attention of members of the press. For example, Warren's wedding to a senator's daughter received media coverage in 1883.[1] As can be seen below, the authors are concerned about the changing norms of the press, as well as a new tool the media had at its disposal: a camera capable of taking photos in an instant.

[1] Amy Gajda, *What If Samuel D. Warren Hadn't Married A Senator's Daughter?: Uncovering the Press Coverage That Led to "The Right to Privacy"*, 2008 MICH. ST. L. REV. 35 (2008).

Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, — the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession — intangible, as well as tangible.

Thus, with the recognition of the legal value of sensations, the protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in fear of such injury. From the action of battery grew that of assault. Much later there came a qualified protection of the individual against offensive noises and odors, against dust and smoke, and excessive vibration. The law of nuisance was developed. So regard for human emotions soon extended the scope of personal immunity beyond the body of the individual. His reputation, the standing among his fellow-men, was considered, and the law of slander and libel arose. Man's family relations became a part of the legal conception of his life, and the alienation of a wife's affections was held remediable. Occasionally the law halted, — as in its refusal to recognize the intrusion by seduction upon the honor of the family. But even here the demands of society were met. A mean fiction, the action *per quod servitium amisit*, was resorted to, and by allowing damages for injury to the parents' feelings, an adequate remedy was ordinarily afforded. Similar to the expansion of the right to life was the growth of the legal conception of property. From corporeal property arose the incorporeal rights issuing out of it; and then there opened the wide realm of intangible property, in the products and processes of the mind, as works of literature and art, goodwill, trade secrets, and trademarks.

This development of the law was inevitable. The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature.

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer. The alleged facts of a somewhat notorious case brought before an inferior tribunal in New York a few months ago, directly involved the consideration of the right of circulating portraits; and the question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration.

Of the desirability — indeed of the necessity — of some such protection, there can, it is believed, be no doubt. The press is overstepping in every direction the obvious bounds of

propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle. The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. Nor is the harm wrought by such invasions confined to the suffering of those who may be made the subjects of journalistic or other enterprise. In this, as in other branches of commerce, the supply creates the demand. Each crop of unseemly gossip, thus harvested, becomes the seed of more, and, in direct proportion to its circulation, results in a lowering of social standards and of morality. Even gossip apparently harmless, when widely and persistently circulated, is potent for evil. It both belittles and perverts. It belittles by inverting the relative importance of things, thus dwarfing the thoughts and aspirations of a people. When personal gossip attains the dignity of print, and crowds the space available for matters of real interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance. Easy of comprehension, appealing to that weak side of human nature which is never wholly cast down by the misfortunes and frailties of our neighbors, no one can be surprised that it usurps the place of interest in brains capable of other things. Triviality destroys at once robustness of thought and delicacy of feeling. No enthusiasm can flourish, no generous impulse can survive under its blighting influence.

It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is.

Owing to the nature of the instruments by which privacy is invaded, the injury inflicted bears a superficial resemblance to the wrongs dealt with by the law of slander and of libel, while a legal remedy for such injury seems to involve the treatment of mere wounded feelings, as a substantive cause of action. The principle on which the law of defamation rests, covers, however, a radically different class of effects from those for which attention is now asked. It deals only with damage to reputation, with the injury done to the individual in his external relations to the community, by lowering him in the estimation of his fellows. The matter published of him, however widely circulated, and however unsuited to publicity, must, in order to be actionable, have a direct tendency to injure him in his intercourse with others, and even if in writing or in print, must subject him to the hatred, ridicule, or contempt of his fellow-men, — the effect of the publication upon his estimate of himself and upon his own feelings not forming an essential element in the cause of action. In short, the wrongs and correlative rights recognized by the law of slander and libel are in their nature material rather than spiritual. That branch of the law simply extends the protection surrounding physical property to certain of the conditions necessary or helpful to worldly prosperity. On the other hand, our law recognizes no principle upon which compensation can be granted for mere injury to the feelings. However painful the mental effects upon another of an act, though purely wanton or even malicious, yet if the act itself is otherwise lawful, the suffering inflicted is *damnum absque injuria.* Injury of feelings may indeed be taken account of in ascertaining the amount of damages when attending what is recognized as a legal injury; but our system, unlike the Roman law, does not afford a remedy even for mental suffering which results from mere contumely and insult, from an intentional and unwarranted violation of the "honor" of another.

It is not however necessary, in order to sustain the view that the common law recognizes and upholds a principle applicable to cases of invasion of privacy, to invoke the analogy, which is but superficial, to injuries sustained, either by an attack upon reputation or by what the

civilians called a violation of honor; for the legal doctrines relating to infractions of what is ordinarily termed the common-law right to intellectual and artistic property are, it is believed, but instances and applications of a general right to privacy, which properly understood afford a remedy for the evils under consideration.

The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Under our system of government, he can never be compelled to express them (except when upon the witness-stand); and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them. The existence of this right does not depend upon the particular method of expression adopted. It is immaterial whether it be by word or by signs, in painting, by sculpture, or in music. Neither does the existence of the right depend upon the nature or value of the thought or emotion, nor upon the excellence of the means of expression. The same protection is accorded to a casual letter or an entry in a diary and to the most valuable poem or essay, to a botch or daub and to a masterpiece. In every such case the individual is entitled to decide whether that which is his shall be given to the public.

What is the nature, the basis, of this right to prevent the publication of manuscripts or works of art? It is stated to be the enforcement of a right of property; and no difficulty arises in accepting this view, so long as we have only to deal with the reproduction of literary and artistic compositions. They certainly possess many of the attributes of ordinary property: they are transferable; they have a value; and publication or reproduction is a use by which that value is realized. But where the value of the production is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all, it is difficult to regard the right as one of property, in the common acceptation of that term. A man records in a letter to his son, or in his diary, that he did not dine with his wife on a certain day. No one into whose hands those papers fall could publish them to the world, even if possession of the documents had been obtained rightfully; and the prohibition would not be confined to the publication of a copy of the letter itself, or of the diary entry; the restraint extends also to a publication of the contents. What is the thing which is protected? Surely, not the intellectual act of recording the fact that the husband did not dine with his wife, but that fact itself. It is not the intellectual product, but the domestic occurrence. A man writes a dozen letters to different people. No person would be permitted to publish a list of the letters written. If the letters or the contents of the diary were protected as literary compositions, the scope of the protection afforded should be the same secured to a published writing under the copyright law. But the copyright law would not prevent an enumeration of the letters, or the publication of some of the facts contained therein. The copyright of a series of paintings or etchings would prevent a reproduction of the paintings as pictures; but it would not prevent a publication of a list or even a description of them.

That this protection cannot rest upon the right to literary or artistic property in any exact sense, appears the more clearly when the subject-matter for which protection is invoked is not even in the form of intellectual property, but has the attributes of ordinary tangible property. Suppose a man has a collection of gems or curiosities which he keeps private: it would hardly be contended that any person could publish a catalogue of them, and yet the articles enumerated are certainly not intellectual property in the legal sense, any more than a collection of stoves or of chairs.

These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed — and (as that is the distinguishing attribute of property) there

may be some propriety in speaking of those rights as property. But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.

If we are correct in this conclusion, the existing law affords a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds.

In Pollard *v.* Photographic Co., 40 Ch. Div. 345 (1888), a photographer who had taken a lady's photograph under the ordinary circumstances was restrained from exhibiting it, and also from selling copies of it, on the ground that it was a breach of an implied term in the contract, and also that it was a breach of confidence. Mr. Justice North interjected in the argument of the plaintiff's counsel the inquiry: "Do you dispute that if the negative likeness were taken on the sly, the person who took it might exhibit copies?" and counsel for the plaintiff answered: "In that case there would be no trust or consideration to support a contract." Later, the defendant's counsel argued that "a person has no property in his own features; short of doing what is libellous or otherwise illegal, there is no restriction on the photographer's using his negative." But the court, while expressly finding a breach of contract and of trust sufficient to justify its interposition, still seems to have felt the necessity of resting the decision also upon a right of property, in order to bring it within the line of those cases which were relied upon as precedents.

This process of implying a term in a contract, or of implying a trust (particularly where the contract is written, and where there is no established usage or custom), is nothing more nor less than a judicial declaration that public morality, private justice, and general convenience demand the recognition of such a rule, and that the publication under similar circumstances would be considered an intolerable abuse. So long as these circumstances happen to present a contract upon which such a term can be engrafted by the judicial mind, or to supply relations upon which a trust or confidence can be erected, there may be no objection to working out the desired protection through the doctrines of contract or of trust. But the court can hardly stop there. The narrower doctrine may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation. While, for instance, the state of the photographic art was such that one's picture could seldom be taken without his consciously "sitting" for the purpose, the law of contract or of trust might afford the prudent man sufficient safeguards against the improper circulation of his portrait; but since the latest advances in photographic art have rendered it possible to take pictures surreptitiously, the doctrines of contract and of trust are inadequate to support the required protection, and the law of tort must be resorted to. The right of property in its widest sense, including all possession, including all rights and privileges, and hence embracing the right to an inviolate personality, affords alone that broad basis upon which the protection which the individual demands can be rested.

We must therefore conclude that the rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights as against the world; and, as above stated, the principle which has been applied to protect these rights is in reality not the principle of private property, unless that word be used in an extended and unusual sense. The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relations, domestic or otherwise.

If the invasion of privacy constitutes a legal *injuria*, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation.

The right of one who has remained a private individual, to prevent his public portraiture, presents the simplest case for such extension; the right to protect one's self from pen portraiture, from a discussion by the press of one's private affairs, would be a more important and far-reaching one. If casual and unimportant statements in a letter, if handiwork, however inartistic and valueless, if possessions of all sorts are protected not only against reproduction, but against description and enumeration, how much more should the acts and sayings of a man in his social and domestic relations be guarded from ruthless publicity. If you may not reproduce a woman's face photographically without her consent, how much less should be tolerated the reproduction of her face, her form, and her actions, by graphic descriptions colored to suit a gross and depraved imagination.

To determine in advance of experience the exact line at which the dignity and convenience of the individual must yield to the demands of the public welfare or of private justice would be a difficult task; but the more general rules are furnished by the legal analogies already developed in the law of slander and libel, and in the law of literary and artistic property.

> 1. The right to privacy does not prohibit any publication of matter which is of public or general interest.

The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever; their position or station, from having matters which they may properly prefer to keep private, made public against their will. It is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented. The distinction, however, noted in the above statement is obvious and fundamental. There are persons who may reasonably claim as a right, protection from the notoriety entailed by being made the victims of journalistic enterprise. There are others who, in varying degrees, have renounced the right to live their lives screened from public observation. Matters which men of the first class may justly contend, concern themselves alone, may in those of the second be the subject of legitimate interest to their fellow-citizens. Peculiarities of manner and person, which in the ordinary individual should be free from comment, may acquire a public importance, if found in a candidate for political office.

In general, then, the matters of which the publication should be repressed may be described as those which concern the private life, habits, acts, and relations of an individual, and have no legitimate connection with his fitness for a public office which he seeks or for which he is suggested, or for any public or quasi public position which he seeks or for which he is suggested, and have no legitimate relation to or bearing upon any act done by him in a public or quasi public capacity.

> 2. The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel.

Under this rule, the right to privacy is not invaded by any publication made in a court of justice, in legislative bodies, or the committees of those bodies; in municipal assemblies, or the committees of such assemblies, or practically by any communication made in any other public body, municipal or parochial, or in any body quasi public, like the large voluntary associations formed for almost every purpose of benevolence, business, or other general interest; and (at least in many jurisdictions) reports of any such proceedings would in some measure be accorded a like privilege. Nor would the rule prohibit any publication made by one in the discharge of some public or private duty, whether legal or moral, or in conduct of one's own affairs, in matters where his own interest is concerned.

> 3. The law would probably not grant any redress for the invasion of privacy by oral publication in the absence of special damage.

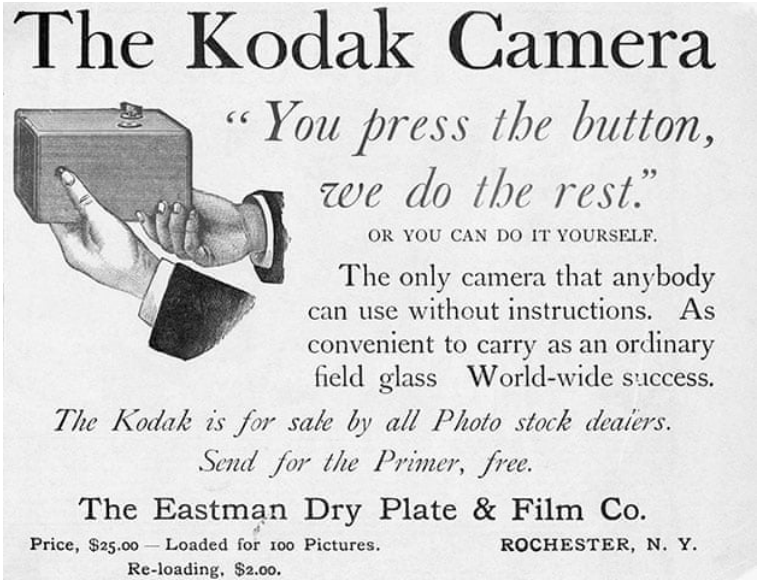
The same reasons exist for distinguishing between oral and written publications of private matters, as is afforded in the law of defamation by the restricted liability for slander as compared with the liability for libel. The injury resulting from such oral communications would ordinarily be so trifling that the law might well, in the interest of free speech, disregard it altogether.

> 4. The right to privacy ceases upon the publication of the facts by the individual, or with his consent.
>
> 5. The truth of the matter published does not afford a defence. Obviously this branch of the law should have no concern with the truth or falsehood of the matters published. It is not for injury to the individual's character that redress or prevention is sought, but for injury to the right of privacy. For the former, the law of slander and libel provides perhaps a sufficient safeguard. The latter implies the right not merely to prevent inaccurate portrayal of private life, but to prevent its being depicted at all.
>
> 6. The absence of "malice" in the publisher does not afford a defence. Personal ill-will is not an ingredient of the offence, any more than in an ordinary case of trespass to person or to property.

It would doubtless be desirable that the privacy of the individual should receive the added protection of the criminal law, but for this, legislation would be required. Perhaps it would be deemed proper to bring the criminal liability for such publication within narrower limits; but that the community has an interest in preventing such invasions of privacy, sufficiently strong to justify the introduction of such a remedy, cannot be doubted. The common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?

Notes

1. Warren and Brandeis's argument is notable for three points:
   a) A fear of how growing technology has enabled invasions of private spaces and moments that were previously inaccessible to the public.
   b) A recognition that this technological change enables observation and photography of people by strangers, reducing the ability to protect privacy via contract.
   c) An acknowledgement that some privacy invasions must be permissible in a free and democratic society in order to promote the public discourse.
2. The key technology in question here is the Kodak Camera of 1888. It allowed for a photographer to take a photograph in an instant, hence "instantaneous photography." Prior to this invention, photography was a matter of posed pictures, with the subject needing to hold still and therefore be at least somewhat cooperative. Afterward, it was possible to take a photo of a moving person, meaning that the person need not cooperate.



3. One key question is what information should count as *newsworthy*. Warren and Brandeis recognize that the public needs more information about those who hold, or seek to hold, the public trust. But what is the limit as to what information the public should have about such people? Or is there a limit? The late 20th century saw great interest in the morality of American public figures. If a politician could not be faithful to their spouse, then how could they be trusted to be faithful to the American people? If they could not successfully guide their children, how could they guide their country? This kind of thinking would lead to the conclusion that even the most intimate details of a public official's life are newsworthy. Notably this argument has appeared less often during the early 21st century.
4. Part of Warren's motivation for writing may have been unwanted media coverage about his wedding. Historically, marriage was perceived as squarely on the "private" side of a public/private distinction. For example, in Aristotle's *The Politics*, he distinguished "between the polis, or political realm, and the oikos, or domestic realm. The political realm of governing, open to men only, was deemed by Aristotle to be a public arena, whereas the domestic realm of home and family was viewed by him to be a private arena."[2] While some aspects of Aristotle's theory are clearly outdated, his idea of a public/private distinction has continued to guide much of privacy law scholarship. How has the perception of marriage as private changed—or failed to change—over time? Consider, for example, the Office of the First Lady or First Gentleman, which has a full-time, federally-funded staff. What are some implications of a public/private distinction rooted in traditional gender roles?
5. Warren and Brandeis are particularly concerned about the problem of an overzealous press. But now anyone can easily publish to the world on social media. Does this mean that the problem is magnified, with more people potentially set to invade privacy? Or should the democratization of access to publication make us more hesitant to regulate privacy as they suggest?

[2] Judith Wagner DeCew, *The Feminist Critique of Privacy: Past Arguments and New Social Understandings*, 88, in SOCIAL DIMENSIONS OF PRIVACY (Cambridge: Roessler & Mokrosinska eds. 2015).

B. Privacy values – What is privacy and why is it important?

Privacy means different things to different people, and even to the same people at different times and in different contexts. In the 1960s and 70s, the biggest privacy cases tended to involve matters of what are now termed "decisional privacy," particularly abortion and contraception. Those sorts of issues are still with us today, with the same-sex marriage cases of the 2010s and the overturning of *Roe v. Wade* in *Dobbs v. Jackson Women's Health Organization* (2022). But now these sexual autonomy questions are joined by an array of concerns related to information privacy in the electronic age. These range from the growth of Big Data in the consumer law domain, to the use of employee background checks, to the National Security Agency's collection of telephone metadata.

It is difficult, however, to draw clear connections between some of these different privacy domains. Is there an inherent link between the government's ability to prohibit first-trimester abortions and a company's ability to repurpose consumer data for advertising? Should judges thinking about a new issue in criminal procedure, such as the use of a GPS tracking device, be asking the same types of questions about societal chilling effects and personal autonomy as they might in a case about employee privacy?

One could easily argue that these domains are largely distinct. Lior Strahilevitz, for example, observes that "the stark differences in the respective analytical frameworks, stakes, historical pedigrees, and distributive contexts dwarf the extant similarities between informational and decisional privacy."[3] And, even within the comparatively smaller and more homogenous domain of information privacy, Daniel Solove has argued that "[p]rivacy is a concept in disarray,"[4] representing a mass of conflicting doctrines from tort law, criminal procedure, and First Amendment jurisprudence that have no common core.[5]

Nevertheless, some scholars have argued that these different privacy domains are unified by themes such as the creation of individual comfort, the protection of individual autonomy, the promotion of intimacy, and the preservation of a democratic society. From these perspectives, most or all of privacy law is driven by a desire to protect certain common values. To the extent that these perspectives are correct, it would be highly sensible to use the doctrines of one privacy domain to inform those of others; all privacy jurisprudence would be best viewed as part of a common mission.

1) Privacy's individual function

> *As examples mount of the uses made of the new technology, worried protests against "Big Brother" have set alarms ringing along the civic-group spectrum from extreme left to radical right. Reflecting this concern, "invasion of privacy" has become a leading topic in law-review articles and social-science journals, as well as the subject of legislative and executive investigations at the state and federal levels and of a growing number of exploratory judicial rulings throughout the country . . . .*[6]

---

[3] Lior J. Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007, 2009 (2010).
[4] Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).
[5] *Id.* at 480–82.
[6] Alan F. Westin, *Privacy and Freedom* 1 (1967).

The above was written in 1967. It could just as easily have been written in 1977, 1987, or 2027. With the advent of the computer revolution of the 1960s,[7] there was increasing concern about the ease with which information could be collected and analyzed. Imagine a world in which every adult has a paper record, perhaps of their taxes, on file with the government. This record is stored in a warehouse and can be accessed with much difficulty by having a person physically search for it among tens of thousands of others. Now imagine that those records are computerized. That same record can be obtained in seconds with trivial effort. More, a search can be run to identify which records, of the thousands in the government's possession, meet certain criteria. The world suddenly looks a lot smaller.

Central to the development of American privacy thinking during these earliest years of the data revolution was the work of Alan Westin. His book *Privacy and Freedom* helped form the foundation of much of what followed. He outlined four primary functions of privacy: personal autonomy, emotional release, self-evaluation, and protected communication. These blend into each other, but provide a useful starting point for discussion.

Alan Westin, Privacy and Freedom (1967)

Personal Autonomy. In democratic societies there is a fundamental belief in the uniqueness of the individual, in his basic dignity and worth as a creature of God and a human being, and in the need to maintain social processes that safeguard his sacred individuality. Psychologists and sociologists have linked the development and maintenance of this sense of individuality to the human need for autonomy—the desire to avoid being manipulated or dominated wholly by others . . . .

The most serious threat to the individual's autonomy is the possibility that someone may penetrate the inner zone and learn his ultimate secrets, either by physical or psychological means. This deliberate penetration of the individual's protective shell, his psychological armor, would leave him naked to ridicule and shame and would put him under the control of those who knew his secrets. . . . Each person is aware of the gap between what he wants to be and what he actually is, between what the world sees of him and what he knows to be his much more complex reality. In addition, there are aspects of himself that the individual does not fully understand but is slowly exploring and shaping as he develops. Every individual lives behind a mask in this manner; indeed, the first etymological meaning of the word "person" was "mask," indicating both the conscious and expressive presentation of the self to a social audience. If this mask is torn off and the individual's real self bared to a world in which everyone else still wears his mask and believes in masked performances, performances, the individual can be seared by the hot light of selective, forced exposure. . . . Leontine Young has noted that "without privacy there is no individuality. There are only types. Who can know what he thinks and feels if he never has the opportunity to be alone with his thoughts and feelings?"

Emotional Release. Life in society generates such tensions for the individual that both physical and psychological health demand periods of privacy for various types of emotional release. At one level, such relaxation is required from the pressure of playing social roles. Social scientists agree that each person constantly plays a series of varied and multiple roles, depending on his audience and behavioral situation. On any given day a man may move through the roles of stern father, loving husband, carpool comedian, skilled lathe operator, union steward, watercooler flirt, and American Legion committee chairman—all psychologically different roles that he adopts as he moves from scene to scene on the social stage. Like actors on the dramatic stage, individuals can sustain roles only for reasonable periods of time, and no

[7] The number of computer revolutions in the past century is humbling. The twenty years prior to 1970 saw the first modern programming languages and the invention of both computer transistors and integrated circuits. An incomplete list of the computer revolutions since 1970 would include the advent of the home computer, the advent of the internet, and the advent of the smartphone.

individual can play indefinitely, without relief, the variety of roles that life demands. There have to be moments "off stage" when the individual can be "himself": tender, angry, irritable, lustful, or dream-filled. Such moments may come in solitude; in the intimacy of family, peers, or woman-to-woman and man-to-man relaxation; in the anonymity of park or street; or in a state of reserve while in a group. Privacy in this aspect gives individuals, from factory workers to Presidents, a chance to lay their masks aside for rest. To be always "on" would destroy the human organism.

Another form of emotional release is provided by the protection privacy gives to minor non-compliance with social norms. Some norms are formally adopted—perhaps as law—which society really expects many persons to break. This ambivalence produces a situation in which almost everyone does break some social or institutional norms—for example, violating traffic laws, breaking sexual mores, cheating on expense accounts, overstating income-tax deductions, or smoking in rest rooms when this is prohibited. Although society will usually punish the most flagrant abuses, it tolerates the great bulk of the violations as "permissible" deviations. If there were no privacy to permit society to ignore these deviations—if all transgressions were known—most persons in society would be under organizational discipline or in jail, or could be manipulated by threats of such action.

Self-Evaluation. Every individual needs to integrate his experiences into a meaningful pattern and to exert his individuality on events. To carry on such self-evaluation, privacy is essential. At the intellectual level, individuals need to process the information that is constantly bombarding them, information that cannot be processed while they are still "on the go." Alan Bates has written that privacy in such circumstances enables a person to "assess the flood of information received, to consider alternatives and possible consequences so that he may then act as consistently and appropriately as possible." Privacy serves not only a processing but a planning need, by providing a time "to anticipate, to recast, and to originate." This is particularly true of creative persons. Studies of creativity show that it is in reflective solitude and even "daydreaming" during moments of reserve that most creative "non-verbal" thought takes place. At such moments the individual runs ideas and impressions through his mind in a flow of associations; the active presence of others tends to inhibit this process . . . . Many studies and autobiographies have described the "creative loneliness" needed by artists and writers to produce their works.

Limited and Protected Communication. The greatest threat to civilized social life would be a situation in which each individual was utterly candid in his communications with others, saying exactly what he knew or felt at all times. The havoc done to interpersonal relations by children, saints, mental patients, and adult "innocents" is legendary. In real life, among mature persons all communication is partial and limited, based on the complementary relation between reserve and discretion that has already been discussed.

Notes

1. These benefits of privacy likely resonate with most readers. After a long day in public, it is often very refreshing to return home and close the door. Time and space for reflection is key for considered thinking and mental health. The self-control and self-censorship of modern professional life are best borne when balanced with freer activities.
2. If Alan Westin is famous for two things, one is *Privacy and Freedom*. The other is his decades of consulting work. Westin conducted a large number of survey studies from which he concluded that most people (55%) were "privacy pragmatists" and only minorities fell into the "privacy fundamentalist" (25%) and "privacy unconcerned" (20%) camps.[8] Privacy

[8] *Opinion Surveys: What Consumers Have to Say About Information Privacy: Hearing Before the Subcomm. on Commerce, Trade & Consumer Prot. of the H. Comm. on Energy & Commerce,* 107th Cong. 15 (2001); *see also* Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 263, 267–68 (2014) (describing and critiquing Westin's consulting work).

> pragmatists "weigh the value to them and society of various business or government programs calling for personal information, examines the relevance and social propriety of the information sought, wants to know the potential risks to privacy or security of their information . . . and then decides whether they will agree or disagree with specific information activities—with their trust in the particular industry or company involved a critical decisional factor."[9] Privacy fundamentalists and the privacy unconcerned believe what the labels imply: the former is highly committed to privacy in all circumstances and the latter largely indifferent to it.
> Because of the context sensitivity of the privacy pragmatists, Westin advocated leaving much of privacy to the marketplace. Let people decide for themselves whether they are comfortable with various programs that potentially infringe on their privacy.

Westin's approach to privacy was extremely popular with corporate America. Leaving something to the marketplace means not passing laws that extensively regulate it, which is historically an industry-friendly position. But Westin's approach has been extensively critiqued on two fronts. First, it is empirically questionable. People generally do not know much about corporate privacy practices and how those practices might impact their lives. Absent that information, and the time, energy, and expertise to process it, people cannot make good privacy choices.[10] So relying on individual initiative has inherent shortcomings. Second, an individual rational actor model can only account for the privacy costs to a particular person. Even if people can make good individual privacy choices for themselves, they may not be able to make good privacy choices for society as a whole.[11]

2) Privacy's societal function

A society with a great deal of privacy looks very different than one without a great deal of privacy. Focusing purely on the individual costs and benefits of privacy readily misses that fact. Julie Cohen and Anita Allen have both written on the problems caused by overlooking the societal consequences of low privacy.

Julie E. Cohen, *Examined Lives*, 52 STAN. L. REV. 1373 (2000)

Prevailing market-based approaches to data privacy policy—including "solutions" in the form of tradable privacy rights or heightened disclosure requirements before consent—treat preferences for informational privacy as a matter of individual taste, entitled to no more (and often much less) weight than preferences for black shoes over brown or red wine over white. But the values of informational privacy are far more fundamental. A degree of freedom from scrutiny and categorization by others promotes important noninstrumental values, and serves vital individual and collective ends.

First, informational autonomy comports with important values concerning the fair and just treatment of individuals within society. From Kant to Rawls, a central strand of Western philosophical tradition emphasizes respect for the fundamental dignity of persons, and a concomitant commitment to egalitarianism in both principle and practice. Advocates of strong data privacy protection argue that these principles have clear and very specific implications for the treatment of personally-identified data: They require that we forbid data-processing

---

[9] Quoted in Hoofnagle & Urban, *supra* note 8, at 268.

[10] Since Westin's work has been so influential in support of the current "notice and choice" privacy regime, many scholars have addressed this point in general. Hoofnagle and Urban do an excellent job picking apart Westin's own findings, however, so their article is a good place to start if one seeks a Westin-focused critique.

[11] For a discussion of more individual level externalities – your poor privacy practices expose my information as well, see Joshua A. T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385 (2015).

practices that treat individuals as mere conglomerations of transactional data, or that rank people as prospective customers, tenants, neighbors, employees, or insureds based on their financial or genetic desirability. The drafters of the European Data Protection Directive agreed with this characterization; the Directive is explicitly grounded in "the fundamental rights and freedoms of natural persons."

Arguably, however, the leap from normative first principles to the European model of fair information practice requires further explanation. In theory, at least, a market model of tradable privacy rights is fully consistent with first-order normative commitments to dignity and equality, in that it treats each individual as an autonomous, rational actor and presumes that all individuals are equally capable of ascertaining and pursuing the goals that will maximize their own happiness. [Yet] individuals experience substantially less choice about data-processing practice, and enjoy substantially less agency, than the rational-actor model predicts.

Autonomous individuals do not spring full-blown from the womb. We must learn to process information and to draw our own conclusions about the world around us. Autonomy in a contingent world requires a zone of relative insulation from outside scrutiny and interference—a field of operation within which to engage in the conscious construction of self. The solution to the paradox of contingent autonomy, in other words, lies in a second paradox: To exist in fact as well as in theory, autonomy must be nurtured.

A realm of autonomous, unmonitored choice, in turn, promotes a vital diversity of speech and behavior. The recognition that anonymity shelters constitutionally-protected decisions about speech, belief, and political and intellectual association—decisions that otherwise might be chilled by unpopularity or simple difference—is part of our constitutional tradition. But the benefits of informational autonomy (defined to include the condition in which no information is recorded about nonanonymous choices) extend to a much wider range of human activity and choice. We do not experiment only with beliefs and associations, but also with every other conceivable type of taste and behavior that expresses and defines self. The opportunity to experiment with preferences is a vital part of the process of learning, and learning to choose, that every individual must undergo.

The benefits of informational privacy are related to, but distinct from, those afforded by seclusion from visual monitoring. It is well-recognized that respite from visual scrutiny affords individuals an important measure of psychological repose. Within our society, at least, we are accustomed to physical spaces within which we can be unobserved, and intrusion into those spaces is experienced as violating the boundaries of self. But the scrutiny, and the repose, can be informational as well as visual, and this does not depend entirely on whether the behavior takes place "in private." The injury, here, does not lie in the exposure of formerly private behaviors to public view, but in the dissolution of the boundaries that insulate different spheres of behavior from one another. The universe of all information about all record-generating behaviors generates a "picture" that, in some respects, is more detailed and intimate than that produced by visual observation, and that picture is accessible, in theory and often in reality, to just about anyone who wants to see it. In such a world, we all may be more cautious.

The point is not that people will not learn under conditions of no-privacy, but that they will learn differently, and that the experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior. Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream. The result will be a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines. But rough edges and sharp lines have intrinsic, archetypal value within our culture. Their philosophical differences aside, the coolly rational Enlightenment thinker, the unconventional Romantic dissenter, the skeptical pragmatist, and the iconoclastic postmodernist all share a deep-rooted antipathy toward unreflective conformism. The condition

of no-privacy threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it.

The autonomy fostered by informational privacy also generates more concrete collective benefits. Development of the capacity for autonomous choice is an indispensable condition for reasoned participation in the governance of the community and its constituent institutions—political, economic, and social.

The cornerstone of a democratic society is informed and deliberate self-governance. The formation and reformation of political preferences—essential both for reasoned public debate and informed exercise of the franchise—follows the pattern already discussed: Examination chills experimentation with the unorthodox, the unpopular, and the merely unfinished. A robust and varied debate on matters of public concern requires the opportunity to experiment with self-definition in private, and (if one desires) to keep distinct social, commercial, and political associations separate from one another. Here again the point is relative. People will still make choices under conditions of no-privacy, and targeted commercial advertising can be used to manufacture political preferences (or political apathy) as well. But if we do not wish to live in communities governed by apathy, impulse, or precautionary conformism, we must produce individuals capable of governing themselves.

At the same time, though, the insulation provided by informational privacy also plays a subtler, more conservative role in reinforcing the existing social fabric. Sociologist Erving Goffman demonstrated that the construction of social facades to mediate between self and community is both instinctive and expected. Alan Westin describes this social dimension of privacy as "reserve." This characterization, though, seems incomplete. On Goffman's account, the construction of social personae isn't just about withholding information that we don't want others to have. It is about defining the parameters of social interaction in ways that maximize social ease, and thus is about collective as well as individual comfort. We do not need, or even want, to know each other that well. Less information makes routine interactions easier; we are then free to choose, consensually and without embarrassment, the interactions that we wish to treat as less routine. Informational privacy, in short, is a constitutive element of a civil society in the broadest sense of that term.

Technological progress affords a yardstick for measuring human achievement, but not the only or most important one. To appreciate other measures of progress, we must be sensitive to the limits of technique, and recognize the hubris inherent in pretensions to total prediction and control. A protected zone of informational autonomy is valuable, in short, precisely because it reminds us what we cannot measure.

Notes

1. Both Westin and Cohen like privacy. Is the difference here that Cohen likes it more, or is there a more fundamental split?
2. Cohen's emphasis on coercion may initially lead one to think that she is predominantly concerned with privacy from government actors. But this is not the case. The coercive effect of private surveillance can also be large. Would students be comfortable with their future employers knowing which protests they attended, which causes they supported, and which topics they researched? Even if the students are proud of their beliefs, they may not want to justify them to future employers or guess at the biases and beliefs every interviewer might hold.
3. Who most needs privacy, in Cohen's view? Presumably the unconventional and the different. A person who golfs is extremely unlikely to suffer negative professional consequences from their hobby becoming known. Depending on environment, however, a person may wish to hide that they are gay, trans, religious, irreligious, politically liberal, politically conservative, or the author of a popular erotic Harry Potter fanfiction. All of these could go over poorly in the wrong environment.

Recognizing that environments vary drives home the ways in which all people need privacy. A person who is in the social majority in their hometown may find themselves a disliked minority on their university campus. Someone whose views are popular among their young peers might be viewed as socially deviant by their senior colleagues. Even our golfer might find themselves judged in the wrong setting.

Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723 (1999)

Some people really care about privacy; my point, however, is that many people do not.

The group that does not care much about privacy may consist of individuals who share some things in common. The regard one has for privacy or particular forms of privacy may be partly a function of one's generation, educational background, and wealth. An upper middle-class person can afford to care about the privacy of her body. She does not need to take a job as a stripper, whereas a poor, uneducated person might. Generational differences in the taste for privacy may be significant in the United States, as younger Americans appear to be learning to live reasonably well and happily without privacy. Young adults seem to take exposure for granted and many understand that they live in virtual glass houses. Anyone with sophistication about the Internet or the credit and insurance industries knows that it is easy and cheap to find out facts about friends, neighbors, and strangers. I may not be able to walk into your bedroom, but I can find out how much you earn, where you work, your Social Security number, and how much you paid for your house. Young adults today understand that their medical records are not seen solely by their doctors, and that cameras posted in workplaces, at ATM machines, and on the public streets monitor their conduct. They know about the night detection devices and hyperbolic microphones that enable others to see and hear inside their homes.

For people under forty-five who understand that they do not, and cannot, expect to have many secrets, informational privacy may now seem less important. As a culture, we seem to be learning how to be happy and productive—even spiritual—knowing that we are like open books, our houses made of glass. Our parents may appear on the television shows of Oprah Winfrey or Jerry Springer to discuss incest, homosexuality, miscegenation, adultery, transvestitism, and cruelty in the family. Our adopted children may go on television to be reunited with their birth parents. Our law students may compete with their peers for a spot on the MTV program The Real World, and a chance to live with television cameras for months on end and be viewed by mass audiences. Our ten-year-olds may aspire to have their summer camp experiences—snits, fights, fun, and all—chronicled by camera crews and broadcast as entertainment for others on the Disney Channel.

Should we worry about any of this? What values are at stake? Scholars and other commentators associate privacy with several important clusters of value. Privacy has value relative to normative conceptions of spiritual personality, political freedom, health and welfare, human dignity, and autonomy.

The formation of self-concept and intimate relationships on which workable family and community life depend, however, requires opportunities for privacy and private choice. Privacy is down time. Privacy allows me to rest, retool, and as a result, better prepare myself for my social responsibilities, whether they be familial, local, or global. Privacy has value as the context in which individuals work to make themselves better equipped for their familial, professional, and political roles. With privacy, I can try to become competent to perform and achieve up to my capacities, as well as to try out new ideas and practice developing skills.

To speak of "coercing" privacy is to call attention to privacy as a foundation, a precondition of a liberal egalitarian society. Privacy is not an optional good, like a second home or an investment account. The argument of this Essay is structurally identical to an argument philosopher Samuel Freeman makes about drug policy. It would be illiberal to criminalize addictive recreational drugs in the absence of good evidence of substantial negative

externalities, were clear-headed cognitive capacity not a requirement of responsible participation in a liberal democratic government. Similarly, it would be illiberal to coerce privacy were something approaching the ideal of morally autonomous selves not a requirement of participation in a liberal democratic society.

A hard task seems to lay before us—namely, deciding which forms of privacy are so critical that they should become matters of coercion. The task is especially hard because we cannot fairly rely solely and uncritically on traditional notions of modesty and civility. Responding to the erosion of privacy tastes and expectations is not just a matter of outlawing nudity on the Internet or demanding standards for broadcasters and publishers that limit the number of confessional television shows and publications. No one is rendered unfit for life in a liberal democracy because he or she posed nude or appeared once on Jerry Springer or Oprah. Yet numerous little consensual and nonconsensual privacy losses, too trivial to protest individually, aggregate into a large privacy loss that is a detriment to the liberal way of life. It is this aggregation problem of cumulative accessibility and accountability to others that policymakers should begin to try to address.

This policymaking task should be guided by a consideration of the cumulative effect of living without "down time" in a seclusion-deficient, access-compulsive world. We live in busy households, with partners, children, and parents who have complete access to us; we walk down busy streets where we are observed and approached by others, and where video cameras may track our moves to deter crime; law enforcers observe and monitor our automobile driving; employers ask for blood and urine samples, and request psychological testing; our supervisors and co-workers may read our mail and e-mail, and listen in on our telephone calls; we make purchases from retailers who bank information about us, sell it to others, and are subject to subpoenas; we travel with cellular phones, beepers, and laptops, and our portable phone conversations can be intercepted by third parties. Approaches to coercing privacy should take all of this experiential reality into account while avoiding the easy assumption, attacked by feminist theory, that social elites know exactly what kinds of privacy and private lives are appropriate for everyone.

Notes

1. Allen worries that people give up privacy too readily given the costs to autonomy and democratic society. In a way, this is a natural extension of Cohen's argument (though Cohen actually writes after Allen).
2. In subsequent work, Allen points out the many ways in which privacy is already forced upon people. Anita Allen, *Unpopular Privacy: What Must We Hide* (Oxford 2011). The Children's Online Privacy Protection Act, for instance, forces privacy on those under 13, even if they wish to disclose personal information to others online. Nudity laws often prohibit both professional and recreational exposure of the body in public settings. And many professionals are prohibited from disclosing confidential information learned in the course of their dealings. Allen examines the merits of paternalistic privacy in these and other cases from a feminist perspective. She notes, for instance, that "history shows that women have fought against lives in the shadows, kept there by privacy-related expectations that they dress modest, stay inside the home, and keep their mouths shut."
3. Is Allen right that people do not value privacy enough? Or is Allen missing something with her concerns about the late-1990s equivalent of social media? Is the problem that people here are getting the amount of privacy that they want—and that Allen thinks that amount is too low—or that people are not getting as much privacy as they want?
4. Other scholars—many writing from a feminist perspective—are less favorable toward the notion of involuntary privacy. For example, Susan Moller Okin writes "The protection of the

privacy of a domestic sphere in which inequality exists is the protection of the right of the strong to exploit and abuse the weak."[12] And Catharine MacKinnon wrote:

> For women the measure of the intimacy has been the measure of the oppression. This is why feminism has had to explode the private. This is why feminism has seen the personal as the political. The private is public for those for whom the personal is political. In this sense, for women there is no private, either normatively or empirically. Feminism confronts the fact that women have no privacy to lose or to guarantee. Women are not inviolable. Women's sexuality is not only violable, it is – hence women are – seen in and as their violation. To confront the fact that women have no privacy is to confront the intimate degradation of women as the public order. The doctrinal choice of privacy in the abortion context thus reaffirms and reinforces what the feminist critique of sexuality criticizes: the public/private split.[13]

MacKinnon is arguing that much harm is done to women in private and that keeping many things private perpetuates that harm. What would it look like to "explode" the private and do away with the distinction between public and private? Consider Allen's response to critiques of privacy: "Just as the harm that results from the exercise of individual liberty does not lead to the rejection of liberty, similarly there is inadequate reason to reject privacy completely based on harm done in private."[14] Does her view resolve these concerns?

5. Under Helen Nissenbaum's contextual integrity theory, privacy expectations are "systematically related to characteristics of the background social situation."[15] For example, while privacy is valuable for protecting freedom and comfort in the domestic realm, issues of spousal and child abuse—because they violate existing laws and social norms—warrant government intrusion into an otherwise private space. "The *default* is that privacy protection is fundamental, but considerations of contextual integrity can provide a secondary set of considerations to justify appropriate intervention."[16]

C. Privacy costs – Is privacy good?

Westin, Allen, and Cohen would all agree that privacy is often good. Yet some disagree. The classic piece describing the evils of privacy comes from notable judge and legal scholar Richard Posner. He approached privacy from an economic perspective and came to very different conclusions about its general value.

Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978)

The demand for private information (viewed, as it will be throughout this Article, as an intermediate rather than final good) is readily comprehensible where the existence of an actual or potential relationship, business or personal, creates opportunities for gain by the demander. This is obviously true of the information which the tax collector, fiancé, partner, creditor, and competitor, among others, seek. Less obviously, much of the casual prying (a term used here without any pejorative connotation) into the private lives of friends and colleagues that is so common a feature of social life is also motivated, to a greater extent than we may realize, by

---

[12] Susan Mollin Okin, JUSTICE, GENDER, AND THE FAMILY, 174 (1989).

[13] Catharine MacKinnon, TOWARD A FEMINIST THEORY OF THE STATE, 191 (1989).

[14] Anita Allen, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY, 40 (1988).

[15] Helen Nissenbaum, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE, 129 (2010).

[16] Judith Wagner DeCew, *The Feminist Critique of Privacy: Past Arguments and New Social Understandings*, in SOCIAL DIMENSIONS OF PRIVACY (Cambridge: Roessler & Mokrosinska eds. 2015).

rational considerations of self-interest. Prying enables one to form a more accurate picture of a friend or colleague, and the knowledge gained is useful in one's social or professional dealings with him. For example, in choosing a friend one legitimately wants to know whether he will be discreet or indiscreet, selfish or generous, and these qualities are not always apparent on initial acquaintance. Even a pure altruist needs to know the (approximate) wealth of any prospective beneficiary of his altruism in order to be able to gauge the value of a transfer to him.

The other side of the coin is that social, like business, dealings present opportunities for exploitation through misrepresentation. Psychologists and sociologists have pointed out that even in everyday life people try to manipulate by misrepresentation other people's opinion of them. As one psychologist has written, the "wish for privacy expresses a desire . . . to control others' perceptions and beliefs vis-à-vis the self-concealing person." Even the strongest defenders of privacy describe the individual's right to privacy as the right to "control the flow of information about him." A seldom remarked corollary to a right to misrepresent one's character is that others have a legitimate interest in unmasking the deception.

Yet some of the demand for private information about other people is not self-protection in the foregoing sense but seems mysteriously disinterested—for example, that of the readers of newspaper gossip columns, whose "idle curiosity" Warren and Brandeis deplored, groundlessly in my opinion. Gossip columns recount the personal lives of wealthy and successful people whose tastes and habits offer models—that is, yield information—to the ordinary person in making consumption, career, and other decisions. The models are not always positive. The story of Howard Hughes, for example, is usually told as a morality play, warning of the pitfalls of success. Tales of the notorious and the criminal—of Profumo and of Leopold—have a similar function. Gossip columns open people's eyes to opportunities and dangers; they are genuinely informational.

The expression "idle curiosity" is misleading. People are not given to random, undifferentiated curiosity. Why is there less curiosity about the lives of the poor (as measured, for example, by the frequency with which poor people figure as central characters in novels) than about those of the rich? The reason is that the lives of the poor do not provide as much useful information in patterning our own lives. What interest there is in the poor is focused on people who are (or were) like us but who became poor rather than on those who were always poor; again the cautionary function of such information should be evident.

Warren and Brandeis attributed the rise of curiosity about people's lives to the excesses of the press. The economist does not believe, however, that supply creates demand. A more persuasive explanation for the rise of the gossip column is the secular increase in personal incomes. There is apparently very little privacy in poor societies, where, consequently, people can easily observe at first hand the intimate lives of others. Personal surveillance is costlier in wealthier societies both because people live in conditions that give them greater privacy from such observation and because the value (and hence opportunity cost) of time is greater—too great to make a generous allotment of time to watching neighbors worthwhile. People in the wealthier societies sought an alternative method of informing themselves about how others live and the press provided it. A legitimate and important function of the press is to provide specialization in prying in societies where the costs of obtaining information have become too great for the Nosey Parker.

The type of private information discussed thus far is not, in general, discreditable to the individual to whom it pertains. Yet we have seen that there may still be good reasons to assign the property right away from him. Much of the demand for privacy, however, concerns discreditable information, often information concerning past or present criminal activity or moral conduct at variance with a person's professed moral standards. And often the motive for concealment is, as suggested earlier, to mislead those with whom he transacts. Other private information that people wish to conceal, while not strictly discreditable, would if revealed correct misapprehensions that the individual is trying to exploit, as when a worker conceals a

serious health problem from his employer or a prospective husband conceals his sterility from his fiancée. It is not clear why society should assign the property right in such information to the individual to whom it pertains; and the common law, as we shall see, generally does not.

An analogy to the world of commerce may help to explain why people should not—on economic grounds, in any event—have a right to conceal material facts about themselves. We think it wrong (and inefficient) that the law should permit a seller in hawking his wares to make false or incomplete representations as to their quality. But people "sell" themselves as well as their goods. They profess high standards of behavior in order to induce others to engage in social or business dealings with them from which they derive an advantage but at the same time they conceal some of the facts that these acquaintances would find useful in forming an accurate picture of their character. There are practical reasons for not imposing a general legal duty of full and frank disclosure of one's material personal shortcomings—a duty not to be a hypocrite. But everyone should be allowed to protect himself from disadvantageous transactions by ferreting out concealed facts about individuals which are material to the representations (implicit or explicit) that those individuals make concerning their moral qualities.

It is no answer that such individuals have "the right to be let alone." Very few people want to be let alone. They want to manipulate the world around them by selective disclosure of facts about themselves. Why should others be asked to take their self-serving claims at face value and be prevented from obtaining the information necessary to verify or disprove these claims?

Some private information that people desire to conceal is not discreditable. In our culture, for example, most people do not like to be seen naked, quite apart from any discreditable fact that such observation might reveal. I do not think, however, that many people have a *general* reticence that makes them wish to conceal nondiscrediting personal information. Anyone who has ever sat next to a stranger on an airplane or a ski lift knows the delight that people take in talking about themselves to complete strangers. Reticence comes into play when one is speaking to people—friends, relatives, acquaintances, business associates—who might use information about him to gain an advantage in some business or social transaction with him. Reticence is generally a means rather than an end.

The reluctance of many people to reveal their income is sometimes offered as an example of a desire for privacy that cannot be explained in purely instrumental terms. But I suggest that people conceal an unexpectedly low income because being thought to have a high income has value in credit markets and elsewhere, and that they conceal an unexpectedly high income in order (1) to avoid the attention of tax collectors, kidnappers, and thieves, (2) to fend off solicitations from charities and family members, and (3) to preserve a reputation for generosity that might be demolished if others knew the precise fraction of their income that they give away. Points (1) and (2) may explain anonymous gifts to charity.

To the extent that people conceal personal information in order to mislead, the economic case for according legal protection to such information is no better than that for permitting fraud in the sale of goods. However, it is also necessary to consider the *means* by which others obtain personal information. Prying by means of casual interrogation of acquaintances of the object of the prying must be distinguished from eavesdropping, electronically or otherwise, on a person's conversations. *A* in conversation with *B* disparages *C*. If *C* has a right to hear this conversation, *A,* in choosing the words he uses to *B,* will have to consider the possible reactions of *C*. Conversation will be more costly because of the external effects, and the increased costs will result in less, and less effective, communication. After people adjust to this new world of public conversation, even the *C*'s of the world will cease to derive much benefit in the way of greater information from conversational publicity, for people will be more guarded in their speech.

The analysis in this section can readily be extended to efforts to obtain people's notes, letters, and other private papers; the efforts would inhibit communication. Photographic surveillance—for example, of the interior of a person's home—presents a slightly more complex question. Privacy enables a person to dress and otherwise disport himself in his home without regard to the effect on third parties. This informality, which is resource-conserving, would be lost were the interior of the home in the public domain. People dress not merely because of the effect on others but also because of the reticence, remarked earlier, concerning nudity and other sensitive states; that reticence is another reason for giving people a privacy right with regard to places in which these sensitive states occur.

Notes

1. In a simplified model, markets work better when there is more information rather than less. If a company can accurately distinguish between the productivity levels of potential employees, it can make offers accordingly. The only benefit to being able to hide information about yourself is to trick people into assigning incorrect—and presumably inflated—value to you. This may be to your benefit, but it comes at a cost to everyone else. Every time an employee hides that they have been fired in the past or a potential romantic partner hides their untreated anger issues, they make the market slightly worse.
   But this theory assumes a high level of rationality and ample time to think and reflect.[17] In a world of bias, people might be consistently and unfairly judged based on irrelevant or outdated information. In such cases, the market might work better if such distracting information were removed. Imagine an employer who thinks that people of a particular race, people from Michigan, or people who like hockey are inherently superior to others. If their belief is incorrect, then hiding such information from them would help rather than hinder their decisionmaking. If their belief is both incorrect and widespread (many people irrationally favor Michigan), then society as a whole would function better were the information hidden.
2. Posner also has a different take on gossip than what we saw from Warren and Brandeis. Gossip, in his view, is good. It tells us about the merits of particular other people and it builds our shared understanding of good and bad conduct. Posner would presumably have approved of the whisper networks in various industries that passed around information about powerful men who engaged in sexual misconduct. Given the merits of gossip that Posner identifies, how can we distinguish between good and bad gossip?
3. Posner is particularly unsympathetic to privacy claims in the national security context. In later work, he wrote, "Privacy is the terrorist's best friend, and the terrorist's privacy has been enhanced by the same technological developments that have both made data mining feasible and elicited vast quantities of personal information from innocents: the internet, with its anonymity, and the secure encryption of digitized data which, when combined with that anonymity, make the internet a powerful tool of conspiracy."[18] This does not make Posner the enemy of all privacy; even in 1978 he wrote about the importance of privacy in communications. But he is sharply appreciative of the benefits of invading privacy, as well as the costs of doing so.
4. Based on the above, one might think that Posner is opposed to all privacy claims. This is not the case. In an opinion in the early 1990s, he wrote:

   > Even people who have nothing rationally to be ashamed of can be mortified by the publication of intimate details of their life. Most people in no way deformed or disfigured would nevertheless be deeply upset if nude photographs of themselves were published in a newspaper or a book. They feel the same way

[17] For a consideration of when people are better at making decisions with less information, see Gerd Gigerenzer and Daniel G. Goldstein, *Reasoning the Fast and Frugal Way: Models of Bounded Rationality*, 103 PSYCH. REV. 650 (1996).

[18] Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. Chi. L. Rev. 245, 251 (2008).

> about photographs of their sexual activities, however "normal," or about a narrative of those activities, or about having their medical records publicized. Although it is well known that every human being defecates, no adult human being in our society wants a newspaper to show a picture of him defecating. The desire for privacy illustrated by these examples is a mysterious but deep fact about human personality. It deserves and in our society receives legal protection.

Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1229 (7th Cir. 1993). How would you describe the kind of privacy that Posner values? Is there any tension between this excerpt and his other writings?

5. Perhaps the best way to assess the disagreement between Posner and privacy advocates is not to ask who is right, but rather who is right *when*. Certain things should generally be disclosed. Other things should generally be hidden. Some information should be disregarded even when it becomes known—the entirety of discrimination law is based on this point. The trick is categorizing different kinds of information. Is it immoral to hide from one's employer that one has cancer and is likely to die within several years? What about hiding that from one's spouse? And should either be illegal? One hot topic in this regard is privacy in criminal records, which will be addressed in a later chapter.

D. Feminist critique

There is no single feminist perspective on privacy. Writers from a feminist perspective do, however, consistently challenge some of the framings used in I.B and I.C. Specifically, it is worth considering how the individual versus societal benefit framing used above fails to account for the below concern about privacy and threats.

Michela Meister and Karen Levy, Digital Security and Reproductive Rights: Lessons for Feminist Cyberlaw (2024)[19]

Dobbs and its aftermath hit home a lesson that feminist security scholars have consistently highlighted: that a good deal of contemporary security research tends to understand digital security threats in relative isolation, devoid of broader context. Academic security scholarship often highlights novel, technically sophisticated digital attacks, yet sometimes neglects the social contexts in which everyday people experience insecurity, and the real, lived consequences of those threats. A new wave of feminist security research has countered this trend, calling explicit attention to the social and relational aspects of digital insecurity—and showing how even technically unsophisticated attacks (which might not traditionally garner much interest among academic security researchers) can be both immensely harmful and extremely difficult to protect against, largely because of their social complexity.

Much of this feminist security scholarship focuses particularly on the context of technology-mediated abuse, an extremely widespread phenomenon which is very likely the most frequent context in which digital insecurity is inexperienced by everyday people. One in three women and one in four men in the United States experiences intimate partner violence, stalking, or rape at some point during their lives, and transgender people are about twice as likely as cisgender people to experience intimate partner violence; digital technologies play a prominent role in abuse contexts, providing means by which attackers can control, stalk, and harass their targets. In this context, the vectors of attack for abuse may be technically very simple and require no special technical expertise—even something as basic as looking over a

[19] In FEMINIST CYBERLAW (Meg Leta Jones and Amanda Levendowski, eds. 2024).

partner's shoulder or perusing search history on a shared device can be sufficient to glean intimate personal data.

A core insight of this line of work is that digital security, while often siloed in academic analysis, is in reality inextricably linked to physical, emotional, sexual, and economic security. Analyzing digital security threats in isolation from other vectors of attack is necessarily incomplete, and often mischaracterizes or understates the potential risks and consequences of digital security breach. For example, traditional digital security research is unlikely to account for the physical proximity of an attacker and a target (which can facilitate involuntary information-sharing, as in shoulder-surfing), the ways in which a target may be have a preexisting relationship with the attacker (giving the attacker access to resources like the answers to common security questions), or the ways in which threats to digital security can go hand-in-hand with threats to other forms of security (for example, an attacker may threaten physical violence if one takes steps to protect one's digital data from access). Feminist thinkers describe how conventional security threat modeling that focuses on digital access in isolation can neglect broader questions about safety and justice for marginalized people.

A similar question of focus arises in legal privacy scholarship. Privacy is sometimes described as having a "dead body problem": many privacy violations lack harms that are readily cognizable as such, making it difficult to address and prevent them through tort law. Targeted ads based on internet tracking, for example, may give one an uneasy feeling of being watched; shoddy privacy practices that result in disclosure of personal information may cause embarrassment or impinge on one's sense of dignity. But unease and humiliation are not concrete harms, and tend not to be readily compensable via tort law. The "dead body problem" in privacy, as it's described, is that there aren't any: the nature of harm is diffuse and abstract, making it difficult to seek legal redress for harms and to marshal the political will to address privacy problems in the policy realm.

Yet feminist thinkers retort: if you can't find any dead bodies in privacy law, you just aren't looking very hard. Feminist legal thinkers have long highlighted in their scholarship the dire, violent, and often life-or-death consequences of privacy and security violation, particularly for women, the LGBTQ community, and communities of color. Perhaps the most direct confrontation between feminist legal thought and "mainline" privacy scholarship arose in 2006, when Ann Bartow wrote an essay reviewing Daniel Solove's *A Taxonomy of Privacy*. Solove's taxonomy, published that same year, has since become one of the most influential and heavily cited articles in all of privacy law; in it, Solove attempts to bring order to the notoriously slippery concept of "privacy" by categorizing privacy violations into sixteen types (aggregation, appropriation, breach of confidentiality, etc.). In her review, Bartow asserts that Solove's taxonomy "suffers from too much doctrine, and not enough dead bodies"; that his "dry, analytical" approach "fail[s] to sufficiently identify and animate the compelling ways that privacy violations can negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease." The diminishment of reproductive rights is one of the chief examples Bartow brings to bear in her critique, noting presciently that "the prospect that women will either forgo sexual relationships or possibly even bear unwanted children as a consequence of inadequate information privacy is the sort of harm Solove's taxonomy could have taken greater notice of."

Solove countered Bartow's critique in a subsequent article, responding that "most privacy problems lack dead bodies." He acknowledges as aberrations ("exceptional cases") a few situations in which women were murdered by stalkers after the stalkers obtained the women's physical addresses from government and commercial sources—but dismisses what he decries as "Bartow's quest for horror stories" as counterproductive. In Solove's view—one that has become as authoritative as that of any contemporary privacy scholar—highlighting the most

visceral and violent privacy harms (it must be noted, those suffered in these cases by women) could serve to obscure other pervasive privacy harms that accrete more gradually and less egregiously. Solove is, of course, correct in assessing that not all privacy harms need to rise to the level of stalking, rape, murder, or forced childbirth to constitute real harms worth addressing. Yet the scholarship also has a performative effect: dismissing these harms as "sensationalistic," as Solove does, sidelines them as distractions from apparently more pressing issues. And it is incontrovertible that the mine run of privacy scholarship has for decades focused a great deal more energy on issues related to consumer protection than it has on issues related to bodily autonomy and physical safety. In part, deciding which harms to name and to most closely associate with the term "privacy" is a question of political strategy, with both benefits and drawbacks; but it certainly bears notice that at least one such drawback is reduced focus, from both scholars and policymakers, on centering reproductive and bodily integrity as a core privacy issue.

The aftermath of *Dobbs* illustrates the inseparability of digital and physical security, and the production of "dead bodies" as a consequence of privacy violation, with stark clarity. Digital vulnerabilities—say, location tracking of one's visit to a reproductive health clinic, or search results demonstrating information-seeking around abortion access—are life-or-death scenarios: they bear directly on the ability to seek lifesaving medical care and to have autonomy over one's own body and future. Digital privacy *is* physical safety in these scenarios, and to isolate it in analysis, without fully accounting for its broader context and effects, necessarily impoverishes both our research and our law. A feminist approach ameliorates this shortcoming through a focus on the inextricability of the digital and the physical, and attention to visceral and violent harm as a key outcome produced by insecurity.

Notes

1. Privacy case law is driven by the interests of those who bring cases. Government agencies tend to go after actors who do a lot of total damage. These are usually big technology companies that do a little bit of harm to millions of people. Private attorneys tend to go after deep pockets with easy and large liabilities. These are, again, often big technology companies. So many who live in the world of privacy litigation and compliance find themselves surrounded by abstract privacy concerns, rarely encountering the concrete "dead bodies" these authors describe. In contrast, very few people can hire a V10 firm when their ex-lover installs a tracking app on their cellphone or leaks their nude photographs. This leads to a host of interesting consequences, including government enforcement against the makers (rather than users) of spyware apps and efforts to establish platform (rather than user) liability for the distribution of nonconsensual pornography.
2. Feminist perspectives on privacy law are many and varied. Privacy is both a tool used by marginalized individuals to protect themselves as well as a shield used by abusers to hide their misconduct. One might have quite different views on how much legal protection to extend to a person's electronic communications, for instance, depending on whether one is concerned with the prosecution of those who commit sexual violence or the protection of those covertly seeking the help of domestic violence shelters.
3. Another note regarding feminist perspectives on privacy involves the topic of family privacy. The privacy of the marital bedroom was invoked in *Griswold v. Connecticut*, one of the foundational cases in the right of privacy jurisprudence. But recognizing family privacy is not without troubling consequences. Reviewing two Supreme Court cases that recognized the rights of parents to direct the education of their children, Barbara Bennett Woodhouse recognized that strong endorsement of parental authority could be used to justify a range of ills, including physical abuse. See Barbara Bennett Woodhouse, *"Who Owns the Child?": Meyer and Pierce and the Child as Property*, 33 WM. & MARY L. REV. 995 (1992). Much evil can happen behind closed doors.

II. Tort privacy and individual privacy actions

A. Intrusion upon seclusion 25
Howard v. Aspen Way Enterprises, Inc., 406 P.3d 1271 (Wyo. 2017) 25
Safari Club International v. Rudolph, 862 F.3d 1113 (9th Cir. 2017) 28
Desnick v. American Broadcasting Companies, Inc., 44 F.3d 1345 (7th Cir. 1995) 33
Council on American-Islamic Relations Action Network, Inc. v. Gaubatz, 793 F.Supp.2d 311 (D.D.C. 2011) 36

B. Public disclosure of private facts 40
1) Elements of public disclosure 40
Finley v. Kelly, 384 F.Supp.3d 898 (M.D. Tenn. 2019) 40
In re Facebook, Inc., Consumer Privacy User Profile Litig., 402 F.Supp.3d 767 (N.D. Cal. 2019) 43
2) Newsworthiness 50
Shulman v. Group W Productions, Inc., 955 P.2d 469 (Cal. 1998) 50
Y.G. v. Jewish Hospital of St. Louis, 795 S.W.2d 488 (Mo. App. 1990) 57
3) Republisher Immunity 63
Sipple v. Chronicle Publishing Co., 154 Cal.App.3d 1040 (1984) 63
4) First Amendment Limitations on Public Disclosure Liability 67
Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975) 68
The Florida Star v. B.J.F., 491 U.S. 524 (1989) 71
Publius v. Boyer–Vine, 237 F.Supp.3d 997 (E.D. Cal. 2017) 79
Bartnicki v. Vopper, 532 U.S. 514 (2001) 83
Boehner v. McDermott, 484 F.3d 573 (D.C. Cir. 2007) 90

C. False Light and Defamation 95
1) False light 95
2) Defamation 95
Eramo v. Rolling Stone, LLC, 209 F.Supp.3d 862 (W.D. Va. 2016) 96
3) Section 230 as a bar to liability 101
Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997) 102

D. Right of Publicity 107
White v. Samsung Electronics America, Inc. 971 F.2d 1395 (9th Cir. 1992) 109
Young v. NeoCortext, Inc., 690 F. Supp. 3d 1091 (C.D. Cal. 2023) 113

E. Nonconsensual pornography and image-based sexual abuse 119
State v. VanBuren, 214 A.3d 791 (Vt. 2019) 119
15 U.S. Code § 6851 - Civil action relating to disclosure of intimate images 128

This chapter's focus is on the kinds of individual privacy lawsuits that one person can file against another. This is distinct from Chapter 3, on government investigations, because here we are concerned with defendants who are people rather than public entities. It is also distinct from Chapter 9, on consumer privacy, because most often these cases concern individual plaintiffs rather than thousands of consumers. There is, however, a fair amount of overlap in practice.

We begin with the four privacy torts, as conceptualized by William Prosser, along with defamation. We then turns to a variety of privacy causes of action created by state legislatures to supplement these basic torts.

A. Intrusion upon seclusion

The first of the privacy torts is intrusion upon seclusion.

Howard v. Aspen Way Enterprises, Inc., 406 P.3d 1271 (Wyo. 2017)

HILL, Justice.

Plaintiffs individually filed separate claims in circuit court asserting invasion of privacy claims against Aspen Way Enterprises, Inc. (Aspen Way).

Aspen Way owns a rent-to-own franchise in Casper, Wyoming, operating under the name Aaron's Sales and Leasing. Plaintiffs each leased a computer from Aspen Way pursuant to lease-purchase agreements, and in May 2015, Plaintiffs individually filed separate complaints against Aspen Way related to those agreements. The complaints each generally alleged that Aspen Way installed software on Plaintiffs' leased computers, without Plaintiffs' knowledge, that enabled Aspen Way to track the leased computers' locations, remotely activate the computers' webcams, and capture screen shots and key strokes. Based on these allegations, Plaintiffs asserted that claims for invasion of privacy/intrusion upon seclusion and breach of the covenant of good faith and fair dealing.

Plaintiffs ask this Court to recognize a common law cause of action for the invasion of privacy tort defined by the Restatement (Second) of Torts (1977) as intrusion upon seclusion. Aspen Way argues against recognizing a common law cause of action for Plaintiffs' privacy claims, contending that if such a cause of action is to be recognized in Wyoming, it should be created and defined by legislative action. We agree with Plaintiffs that the Restatement cause of action for intrusion upon seclusion is consistent with the value our state places on privacy, and we therefore recognize the tort as part of Wyoming's common law.

The Restatement (Second) of Torts generally defines liability for an invasion of privacy as follows:

> (1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.
>
> (2) The right of privacy is invaded by
>
> > (a) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or
> >
> > (b) appropriation of the other's name or likeness, as stated in § 652C; or
> >
> > (c) unreasonable publicity given to the other's private life, as stated in § 652D; or
> >
> > (d) publicity that unreasonably places the other in a false light before the public, as stated in § 652E.

The strand of the privacy tort Plaintiffs assert, and the one they ask this Court to recognize, is intrusion upon seclusion, which the Restatement defines as follows:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. § 652B.

The comments to the section 652B explain the tort's parameters and the showing required to establish its elements.

a. The form of invasion of privacy covered by this Section does not depend upon any publicity given to the person whose interest is invaded or to his affairs. It consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.

b. The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff's room in a hotel or insists over the plaintiff's objection in entering his home. It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires. It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.

c. The defendant is subject to liability under the rule stated in this Section only when he has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs. Thus there is no liability for the examination of a public record concerning the plaintiff, or of documents that the plaintiff is required to keep and make available for public inspection. Nor is there liability for observing him or even taking his photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye. Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters.

d. There is likewise no liability unless the interference with the plaintiff's seclusion is a substantial one, of a kind that would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object. Thus there is no liability for knocking at the plaintiff's door, or calling him to the telephone on one occasion or even two or three, to demand payment of a debt. It is only when the telephone calls are repeated with such persistence and frequency as to amount to a course of hounding the plaintiff, that becomes a substantial burden to his existence, that his privacy is invaded.

A recent survey of the intrusion upon seclusion claim's recognition in other jurisdictions shows majority support for the Restatement approach to the claim. [37 states follow the Restatement, 5 states recognize intrusion by common law but have not adopted the Restatement, and all but four others have adopted something similar by statute. Wyoming is one of the four states that had not yet decided whether to recognize intrusion].

We turn then to the question of whether this Court should likewise join the majority recognition of the intrusion upon seclusion tort.

When the common law cause of action we are considering is a tort, we begin with our understanding that a tort is a "civil wrong * * *; a breach of a duty that the law imposes on persons who stand in a particular relation to one another." *Black's Law Dictionary* 1717 (10th ed. 2014).

Turning to considerations of policy, Wyoming's commitment to individual privacy interests is well established. In 1936, this Court observed that "[t]he home is a favorite of the law. It is there that the citizen can claim the right of privacy, the right to be let alone, on clear

grounds." We later affirmed this commitment, stating that "we regard highly the federal constitutional guarantees to privacy as well as the right to privacy in Wyoming."

We also understand, however, that constitutional protections limit government rather than private intrusions.

The Wyoming legislature has recognized the need to protect its citizens' privacy interests and has acted on this need. *See, e.g.*, Wyo. Stat. Ann. § 16-4-203(d)(xi) (exempting from public disclosure records "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"); Wyo. Stat. Ann. § 6-4-304(a) (criminalizing the act of "looking in a clandestine, surreptitious, prying or secretive nature into an enclosed area where the person being viewed has a reasonable expectation of privacy"); Wyo. Stat. Ann. 6-6-103(b)(i) (criminalizing the making of repeated, anonymous telephone calls that disturb the privacy of persons where the calls were received); Wyo. Stat. Ann. 6-3-504(a)(i) (criminalizing act of knowingly and without authorization accessing a computer, computer system, or computer network) . . . .

Given our state's policy favoring privacy interests and the legislative enactments protecting those interests, we find the tort of intrusion upon seclusion to be well adapted to our circumstances and state of society. It is therefore appropriate to recognize the tort as part of Wyoming's common law. We also agree with Plaintiffs that the Restatement version of the tort is the approach best suited to our common law.

The circuit court granted summary judgment to Aspen Way without determining whether there existed any genuine issues of material fact with respect to Plaintiffs' privacy claims. There have been no factual findings in this case with regard to either the elements of the intrusion upon seclusion tort or Plaintiffs' claimed damages. Without the context provided by the required factual findings, any determination we might make concerning application of the Restatement provisions to this case would be at risk of being imprecise and speculative. It is thus premature for this Court to make any determinations concerning application of the Restatement provisions to Plaintiffs' claims . . . .

Notes

1. *Howard* is useful in that it spends a great deal of time reflecting on the state of the common law. There is widespread consensus that the tort of intrusion upon seclusion exists. Even in cases where statutory causes of action are alleged, it is quite common to also see an intrusion upon seclusion claim. For instance, consider why statutory claims were likely insufficient here. Though Wyoming has some privacy statutes referenced here, none are exactly on point. Wiretap Act, Stored Communications Act, and Computer Fraud and Abuse Act claims are also possible, but all might have statutory problems. Intrusion, if it exists, lacks the technical details that make everything else so hard.
2. This case does not appear to have generated published opinions on remand. Given everything said about the tort, does Aspen Way appear liable if it installed the software without knowledge and, as alleged, did not remove it when the terms of the contract ended? What would it take to make the intrusion reasonable?
   There are two key tricks that might make an intrusion *more* reasonable here. First, policy-based use limitations on the software. Imagine the software is only activated after a client's payment account is in default and the client has refused attempts to negotiate. That ties the surveillance to the company's legitimate business interest and is certainly more reasonable than the alternative. Second, a written consent form. Absent exceptional cases, people can consent to ambitious invasions of privacy in fine print. One could imagine a term explaining that failure to pay would lead to the activation of monitoring software to aid in the recovery of the computer.

Safari Club International v. Rudolph, 862 F.3d 1113 (9th Cir. 2017)

SEEBORG, District Judge:

Dr. Lawrence P. Rudolph is an award-winning hunter who made his way to the top of Safari Club International ("SCI"), a sport hunting and wildlife conservation organization. Following his term at the helm, various SCI members accused him of official misconduct, stripped him of his awards, and then exiled him permanently from the association. That's when the season opened. Rudolph sued SCI and its president, his friend, John Whipple, whom he assured was named only by virtue of his position at the head of the organization. With his quarry in sight, Rudolph lured Whipple to lunch, brought up the pending litigation, recorded the conversation surreptitiously, and then posted it on YouTube for public consumption.

Plaintiff–Appellee SCI is a hunting and wildlife conservation organization with roughly 50,000 members and nearly 200 chapters across twenty-six different countries. Defendant–Appellant Rudolph has been an SCI member for approximately twenty-five years and became a lifetime member of the organization in 2006. Rudolph has occupied a number of organizational positions throughout his tenure with SCI, culminating in consecutive one-year terms as President of SCI and the Safari Club International Foundation ("SCIF").

Following his second year at the helm of the group, Rudolph was hired to perform public relations as the Chief Communications Officer of SCI. In 2012, however, a conflict arose between Rudolph and the organization, with various members accusing him of, among other things, adultery, making false statements, and intellectual property infringement. SCI terminated Rudolph's contract, stripped him of his awards, and expelled him from membership. Whipple was president of SCI at the time of Rudolph's expulsion and signed the letter officially terminating Rudolph's membership

Stung and defiant, Rudolph sued SCI and several of its board members, including Whipple, in November 2012 in the U.S. District Court for the Western District of Pennsylvania. The court dismissed the individual defendants on jurisdictional grounds and Rudolph thereupon refiled the lawsuit against the same individuals in the U.S. District Court for the District of Wyoming. These actions center on Rudolph's claims that SCI members defamed him maliciously in order to ruin his reputation and ultimately to run him out of the organization.

On February 20, 2013, while Whipple was a defendant in the Pennsylvania action, Rudolph invited him to meet for lunch at a restaurant in Los Angeles. At that time, Whipple still considered Rudolph a good friend, and believed Rudolph felt the same way. Indeed, Whipple recalled Rudolph as saying he sued him in Pennsylvania only because he was the current president of SCI. In any event, Whipple said yes and they met at his residence before departing for Wineworks for Everyone, a wine store and restaurant that is open to the general public.

Rudolph and Whipple met over lunch for approximately five hours. There were several other patrons and employees in the restaurant at the time the meeting took place. Whipple offered his own declaration in which he stated that those other patrons in the room were not within earshot of their conversation. He also claimed he and Rudolph kept their voices fairly low, and that when servers approached, they stopped talking about anything substantive. Rudolph, by contrast, insists his recordings demonstrate that the other patrons were close enough to overhear their conversation, and that staff and other patrons repeatedly walked past the table throughout the meeting. Rudolph further claims Whipple never lowered his voice overtly or manifested body language that in any way would suggest he was attempting to maintain privacy or intended to keep the conversation confidential.

Rudolph eventually steered the discussion to the ongoing litigation between himself, Whipple, and SCI. They talked about Whipple's role in the underlying events and the conduct of various SCI board members. Unbeknownst to Whipple, Rudolph recorded both audio and video of the entire conversation ("Whipple Video"), which he later reduced into a film for public

dissemination called: Rudolph v. Safari Club International SCI President Tells the Truth on Video Rudolph Exonerated!! ("Rudolph Video"). The Rudolph Video allegedly contains clips confirming the allegations against Rudolph were false and malicious. Importantly, Rudolph never asked for, nor obtained, Whipple's consent to record the conversation, and Whipple maintained he never would have given Rudolph his consent.

Rudolph posted both videos on YouTube for public viewing, with SCI members being the target audience. Rudolph claims he created the videos for use in his litigation against SCI and various SCI board members, to inform SCI members about the details of the actions, to repair his reputation, and to stop those in power at SCI from wasting SCI's resources.

Section 632 [of the California Penal Code] renders liable "[e]very person who, intentionally and without the consent of all parties to a confidential communication . . . eavesdrops upon or records the confidential communication" by "means of any electronic amplifying or recording device." The term "confidential communication" includes:

> any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but *excludes* a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.

The California Supreme Court found "a conversation is confidential under section 632 if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded."

The Whipple declaration makes out a prima facie case for a violation of section 632, and furnishes an evidentiary basis sufficient for a jury to find in plaintiffs' favor. Though there were "5 to 10 other patrons in the room," Whipple testified the conversation "was not capable of being heard," and noted "any time a waiter or patron came to or by the table, we stopped talking about anything of substance." Whipple then declared he never consented to any recording of the conversation, but learned Rudolph recorded the entire discussion by audio and video means. These allegations, if ultimately proven, reflect that Rudolph recorded the conversation without Whipple's consent, in circumstances under which Whipple reasonably could expect his statements would not be overheard. Accordingly, a reasonable jury could find in plaintiffs' favor should they credit Whipple's declaration.

Rudolph fires off four arguments aimed at upending this conclusion, each of which misses the mark. First, Rudolph submits plaintiffs present no evidence the communication was confidential because the Whipple declaration relates exclusively to Whipple's subjective beliefs. Yet, Whipple was a firsthand participant in the conversation and his declaration speaks not only to his beliefs, but to the objective circumstances surrounding the discussion at the restaurant.

Second, Rudolph submits the unedited Whipple Video defeats the declaration because it proves there can be no objectively reasonable expectation the conversation was confidential. This argument misconstrues the task the parties presented to the district court, for it asks for an explicit weighing of evidence—i.e., the declaration versus the video. The video does not defeat the Whipple declaration as a matter of law because, as the district court found, what one person might consider a normal pause when speaking to a waiter, another could reasonably find to be a deliberate effort to maintain confidentiality.

Third, Rudolph insists as a matter of law there can be no objectively reasonable expectation of confidentiality because the conversation occurred in a place that was open to the public. That contention is at odds with California authority viewing privacy as relative. For instance, in *Lieberman v. KCOP Television, Inc.* (2003), the reporter posing as a patient brought

a companion into the examination room, and later argued the doctor could not expect his communications would be confidential because another person was present. The court found "[t]he presence of others does not necessarily make an expectation of privacy objectively unreasonable, but presents a question of fact for the jury to resolve." The court concluded a jury could find the doctor reasonably expected the communications were private. Likewise, here, if a jury credits the Whipple declaration, it could find Whipple's claimed expectation of privacy to be objectively reasonable. [Fourth argument omitted.]

Rudolph maintains this analysis is flawed, but the authority he invokes does not establish conversations in public locations categorically cannot be confidential. Nor does *Wilkins v. National Broadcasting Company, Inc.* (1999) support a *per se* rule. In that case, two reporters surreptitiously recorded a lunch meeting with two salesmen on "an outside patio table at a restaurant in Malibu." Far from holding that the public setting automatically negated any reasonable expectation of privacy, the court examined the facts surrounding the lunch at length. It observed the reporters had brought two companions with them but the salesmen never inquired as to the identities of the strangers. In addition, "[w]aiters frequently came to the table, but [the salesman] did not acknowledge them, pause in his sales pitch, or even lower his voice." "On the facts of th[e] case," the court found the salesmen had no objectively reasonable expectation of privacy. Here, by contrast, Whipple contends the conversation could not be overheard, because he and Rudolph lowered their voices overtly when others approached.

In short, even the cases cited by Rudolph demonstrate that whether a communication is confidential is a question of fact normally left to the fact finder.

The final claim is for common law invasion of privacy, which requires "(1) intrusion into a private place, conversation[,] or matter, (2) in a manner highly offensive to a reasonable person."

As to the first element, "the defendant must have 'penetrated some zone of physical or sensory privacy . . . or obtained unwanted access to data' by electronic or other covert means, in violation of the law or social norms." "The second common law element essentially involves a 'policy' determination as to whether the alleged intrusion is 'highly offensive' under the particular circumstances." "Relevant factors include the degree and setting of the intrusion, and the intruder's motives and objectives."

Here, Whipple adequately states and substantiates a claim for common law invasion of privacy. Whipple avers Rudolph's surreptitious recording of their lunchtime discussion intruded unlawfully into his private conversation. He maintains the occurrence was objectively offensive because Rudolph used friendship to lure him to lunch, then secretly recorded their conversation and shared it widely with members of the public. The complaint adds Whipple suffered emotional distress, continues to be humiliated, and fears he will be shunned, avoided, and subjected to ridicule. Though the question is close, we think plaintiffs' proffered evidence, taken as whole, could support a reasonable jury finding that Rudolph's actions constituted a "highly offensive" intrusion into Whipple's privacy.

Rudolph's opening shot once again is to say there is no objectively reasonable expectation of privacy when a conversation takes place in a location that is open to the public. However, as we have already discussed, courts have consistently rejected that assertion.

In *Sanders v. American Broadcast Companies* (1999), for example, a reporter working undercover obtained employment alongside the plaintiff as a telepsychic, giving "readings" to customers over the phone. The reporter then secretly videotaped and recorded interactions with the plaintiff and other psychics using a small hidden camera. The tapings occurred in a large room containing 100 cubicles that were open on one side, open on top, and from which coworkers could be seen and heard. Visitors, however, could not enter this area without permission from the front desk. Ultimately, the plaintiff sued the reporter for violating his privacy after one of his conversations aired on television.

The court began its analysis by noting it has not stated "an expectation of privacy, in order to be reasonable for purposes of the intrusion tort, must be of *absolute* or *complete* privacy." Indeed, "privacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic." Rather, "[t]here are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law." In other words, "privacy . . . is relative," and "[t]he mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone." The court added "the reasonableness of a person's expectation of visual and aural privacy depends not only on who might have been able to observe the subject interaction, but on the identity of the claimed intruder and the means of intrusion."

Applying that framework, the court found "an employee may, under some circumstances, have a reasonable expectation of visual or aural privacy against electronic intrusion by a stranger to the workplace, despite the possibility that the conversations and interactions at issue could be witnessed by coworkers." As to the identity of the intruder, the court noted employees were misled to think the reporter was a colleague, and thus had no reason to suspect their conversations would be recorded for television. Looking at the nature of the intrusion, it found "[t]he possibility of being overheard by coworkers does not, as a matter of law, render unreasonable an employee's expectation that his or her interactions within a nonpublic workplace will not be videotaped in secret by a journalist." Distilling its holding, the court said the tort is not defeated "simply because the events or conversations upon which the defendant allegedly intruded were not completely private from all other eyes and ears."

Rudolph is correct *Sanders* distinguished workplaces "regularly open to entry or observation by the public," and said "any expectation of privacy against press recording is less likely to be deemed reasonable" in those locations. The court did not, however, endorse a *per se* rule holding there is no objectively reasonable expectation of privacy when a conversation takes place in a location that is open to the public. Privacy expectations may be diminished in that scenario, but the court's analysis instructs emphatically that the inquiry requires a fact-based investigation of the precise circumstances. This holding is encapsulated in the pronouncement: "the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law."

That *Sanders* did not endorse a *per se* rule is bolstered by the California Supreme Court's subsequent analysis in *Hernandez v. Hillsides* (2009). There, the court examined the privacy expectations of two employees whose shared office their employer surreptitiously videotaped after hours. It described its analytical framework as "consistent with *Sanders*, which asks whether the employee could be 'overheard or observed' by others when the tortious act allegedly occurred." Applying *Sanders*, the court examined "the physical layout of the area intruded upon, its relationship to the workplace as a whole, and the nature of the activities commonly performed in such places." Again, it acknowledged public locations occupy one end of the privacy spectrum, but it continued to suggest the analysis requires a fact-based inquiry into the precise circumstances. In sum, though there is daylight for Rudolph's argument, a *per se* rule would be at odds with the principles articulated by the California Supreme Court in this area.

The absence of a *per se* rule notwithstanding, the sufficiency of Whipple's allegations in light of *Sanders* must be addressed. To start, the identity of the intruder weighs in Whipple's favor as Rudolph lured him to the lunchtime conversation, saying "he had not wanted to sue" him and did so only because Whipple signed a letter as SCI president. True, Whipple and Rudolph were adversaries in litigation, but Whipple still considered Rudolph to be a good friend, and thus had little reason to suspect his conversation might be recorded. The nature and means of intrusion also weigh in Whipple's favor because the parties sought overtly to keep the conversation quiet, yet Rudolph hoodwinked Whipple by recording it. All told, Whipple has offered evidence sufficient to establish a "probability" that a reasonable jury could agree he

maintained an objectively reasonable expectation of privacy, and that Rudolph's recording invaded a confidential conversation under these particular circumstances.

The next element requires the manner of intrusion be "highly offensive" to a reasonable person, and "sufficiently serious" and unwarranted as to constitute an "egregious breach of the social norms." "Even in cases involving the use of photographic and electronic recording devices, which can raise difficult questions about covert surveillance, 'California tort law provides no bright line on ['offensiveness']; each case must be taken on its facts.'"

Rudolph maintains the surreptitious recording was not highly offensive because it took place in a public restaurant amongst adversaries in pending litigation. As Whipple freely discussed sensitive information about pending litigation between himself and Rudolph, Rudolph insists there was no deception, and thus his conduct cannot possibly rise to the level of highly offensive.

To be sure, Rudolph's conduct seems less "offensive" than that committed in other cases involving surreptitious recordings, but a jury could still find the element is met notwithstanding the public nature of the restaurant. There is no doubt it is more offensive to be recorded while in an area with inherently elevated privacy (home, hospital room, bedroom), but the location, at bottom, simply is one factor incorporated into the analysis. Here, moreover, Whipple was misled into thinking Rudolph was a friend, then had his secretly recorded conversation disseminated widely on the Internet. Furthermore, as the district court noted, such conduct can warrant the imposition of criminal penalties, suggesting the California legislature, and perhaps an ordinary person, would view it to be highly offensive.

Notes

1. There is considerable backstory on Rudolph, Safari Club, and restaurants. In 2016, Rudolph's wife Bianca was hunting with him on safari in Zambia. Rudolph later claimed Bianca accidentally shot herself through the heart with a shotgun while packing it away. The Zambian authorities ruled the death accidental and Rudolph and had the body swiftly cremated.
   Shortly thereafter, Rudolph moved his long-time girlfriend into what had previously been the marital home and collected several million dollars of life insurance. The very public existence of the girlfriend had previously a source of some tension between Rudolph and the Safari Club; he had brought her to a Safari Club convention prior to his wife's death and this had "raised several eyebrows."
   Perhaps unsurprisingly, American authorities were suspicious of Bianca's death. In 2022 Rudolph was convicted of her murder. One critical piece of evidence: a steakhouse bartender testified that he heard Rudolph and his girlfriend arguing over drinks and, in a lull in the loud music, heard Rudolph say "I killed my f------ wife for you!" Rudolph later claimed that he had actually said "They're saying that I killed my f------ wife for you!" The jury was apparently unpersuaded.[20]
2. In litigation, having something declared an issue for the finder of fact is deeply consequential because trial is inherently expensive and risky. Even if the defendant is confident in his interpretation of his video, they still must face the possibility that a jury will disagree and also the certainty that taking the matter to a jury will cost a large amount of money.[21]

---

[20] The full saga of Larry Rudolph's activities is reviewed in Lynsey Eidel, *Where Is Dentist Larry Rudolph Now? Inside His Life 9 Years After Killing His Wife on a Safari,* PEOPLE (July 23, 2025). https://people.com/where-is-dentist-larry-rudolph-now-11775873 (to answer the title's question, "Rudolph is currently serving his life sentence at the United States Penitentiary in Terre Haute, Ind.")

[21] The videos are still available on YouTube. One of them is here, linked at a timestamp when a waiter walks by: https://youtu.be/2aYY0YF4ktA?t=634

3. The Ninth Circuit stresses the highly fact-dependent nature of the privacy analysis here. How predictable is that analysis, in your view? Do you feel you know when it is safe to record a conversation in California? The question of when a person can reasonably expects a conversation to be private arises frequently in wiretap law, and there are few easy answers. Note that California is what is called a two- or all-party consent state – everyone in the conversation must consent to the recording to make it lawful. Other states have one-party consent, meaning that the permission of a single party to a conversation is enough to make a recording legal.

Desnick v. American Broadcasting Companies, Inc., 44 F.3d 1345 (7th Cir. 1995)

POSNER, Chief Judge.

In March of 1993 Entine [of ABC] telephoned Dr. Desnick [owner of an ophthalmic clinic] and told him that *PrimeTime Live* wanted to do a broadcast segment on large cataract practices. The Desnick Eye Center has 25 offices in four midwestern states and performs more than 10,000 cataract operations a year, mostly on elderly persons whose cataract surgery is paid for by Medicare. The complaint alleges . . . that Entine told Desnick that the segment would not be about just one cataract practice, that it would not involve "ambush" interviews or "undercover" surveillance, and that it would be "fair and balanced." Thus reassured, Desnick permitted an ABC crew to videotape the Desnick Eye Center's main premises in Chicago, to film a cataract operation "live," and to interview doctors, technicians, and patients.

Unbeknownst to Desnick, Entine had dispatched persons equipped with concealed cameras to offices of the Desnick Eye Center in Wisconsin and Indiana. Posing as patients, these persons—seven in all—requested eye examinations. Plaintiffs Glazer and Simon are among the employees of the Desnick Eye Center who were secretly videotaped examining these "test patients."

The program aired on June 10. Donaldson introduces the segment by saying, "We begin tonight with the story of a so-called 'big cutter,' Dr. James Desnick . . . . [I]n our undercover investigation of the big cutter you'll meet tonight, we turned up evidence that he may also be a big charger, doing unnecessary cataract surgery for the money." Brief interviews with four patients of the Desnick Eye Center follow. One of the patients is satisfied ("I was blessed"); the other three are not—one of them says, "If you got three eyes, he'll get three eyes." Donaldson then reports on the experiences of the seven test patients. The two who were under 65 and thus not eligible for Medicare reimbursement were told they didn't need cataract surgery. Four of the other five were told they did. Glazer and Simon are shown recommending cataract surgery to them. Donaldson tells the viewer that *PrimeTime Live* has hired a professor of ophthalmology to examine the test patients who had been told they needed cataract surgery, and the professor tells the viewer that they didn't need it—with regard to one he says, "I think it would be near malpractice to do surgery on him." Later in the segment he denies that this could just be an honest difference of opinion between professionals.

An ophthalmic surgeon is interviewed who had turned down a job at the Desnick Eye Center because he would not have been "able to screen who I was going to operate on." He claims to have been told by one of the doctors at the Center (not Glazer or Simon) that "as soon as I reject them [i.e., turn down a patient for cataract surgery], they're going in the next room to get surgery." A former marketing executive for the Center says Desnick took advantage of "people who had Alzheimer's, people who did not know what planet they were on, people whose quality of life wouldn't change one iota by having cataract surgery done." Two patients are interviewed who report miserable experiences with the Center—one claiming that the doctors there had failed to spot an easily visible melanoma, another that as a result of unnecessary cataract surgery her "eye ruptured," producing "running pus." A former employee tells the viewer that Dr. Desnick alters patients' medical records to show they need cataract surgery—for example,

changing the record of one patient's vision test from 20/30 to 20/80—and that he instructs all members of his staff to use pens of the same color in order to facilitate the alteration of patients' records.

The second class of claims in this case concerns, as we said, the methods that the defendants used to create the broadcast segment. There are four such claims: that the defendants committed a trespass in insinuating the test patients into the Wisconsin and Indiana offices of the Desnick Eye Center, that they invaded the right of privacy of the Center and its doctors at those offices (specifically Glazer and Simon), that they violated federal and state statutes regulating electronic surveillance, and that they committed fraud by gaining access to the Chicago office by means of a false promise that they would present a "fair and balanced" picture of the Center's operations and would not use "ambush" interviews or undercover surveillance.

To enter upon another's land without consent is a trespass. The force of this rule has, it is true, been diluted somewhat by concepts of privilege and of implied consent. But there is no journalists' privilege to trespass. And there can be no implied consent in any nonfictitious sense of the term when express consent is procured by a misrepresentation or a misleading omission. The Desnick Eye Center would not have agreed to the entry of the test patients into its offices had it known they wanted eye examinations only in order to gather material for a television exposé of the Center and that they were going to make secret videotapes of the examinations. Yet some cases . . . deem consent effective even though it was procured by fraud. There must be *something* to this surprising result. Without it a restaurant critic could not conceal his identity when he ordered a meal, or a browser pretend to be interested in merchandise that he could not afford to buy. Dinner guests would be trespassers if they were false friends who never would have been invited had the host known their true character, and a consumer who in an effort to bargain down an automobile dealer falsely claimed to be able to buy the same car elsewhere at a lower price would be a trespasser in the dealer's showroom. Some of these might be classified as privileged trespasses, designed to promote competition. Others might be thought justified by some kind of implied consent—the restaurant critic for example might point by way of analogy to the use of the "fair use" defense by book reviewers charged with copyright infringement and argue that the restaurant industry as a whole would be injured if restaurants could exclude critics. But most such efforts at rationalization would be little better than evasions. The fact is that consent to an entry is often given legal effect even though the entrant has intentions that if known to the owner of the property would cause him for perfectly understandable and generally ethical or at least lawful reasons to revoke his consent.

The law's willingness to give effect to consent procured by fraud is not limited to the tort of trespass. The *Restatement* gives the example of a man who obtains consent to sexual intercourse by promising a woman $100, yet (unbeknownst to her, of course) he pays her with a counterfeit bill and intended to do so from the start. The man is not guilty of battery, even though unconsented-to sexual intercourse is a battery. Yet we know that to conceal the fact that one has a venereal disease transforms "consensual" intercourse into battery. Seduction, standardly effected by false promises of love, is not rape, intercourse under the pretense of rendering medical or psychiatric treatment is, at least in most states. It certainly is battery. Trespass presents close parallels. If a homeowner opens his door to a purported meter reader who is in fact nothing of the sort—just a busybody curious about the interior of the home—the homeowner's consent to his entry is not a defense to a suit for trespass. And likewise if a competitor gained entry to a business firm's premises posing as a customer but in fact hoping to steal the firm's trade secrets.

How to distinguish the two classes of case—the seducer from the medical impersonator, the restaurant critic from the meter-reader impersonator? The answer can have nothing to do with fraud; there is fraud in all the cases. It has to do with the interest that the torts in question, battery and trespass, protect. The one protects the inviolability of the person, the other the

inviolability of the person's property. The woman who is seduced wants to have sex with her seducer, and the restaurant owner wants to have customers. The woman who is victimized by the medical impersonator has no desire to have sex with her doctor; she wants medical treatment. And the homeowner victimized by the phony meter reader does not want strangers in his house unless they have authorized service functions. The dealer's objection to the customer who claims falsely to have a lower price from a competing dealer is not to the physical presence of the customer, but to the fraud that he is trying to perpetuate. The lines are not bright—they are not even inevitable. They are the traces of the old forms of action, which have resulted in a multitude of artificial distinctions in modern law. But that is nothing new.

There was no invasion in the present case of any of the specific interests that the tort of trespass seeks to protect. The test patients entered offices that were open to anyone expressing a desire for ophthalmic services and videotaped physicians engaged in professional, not personal, communications with strangers (the testers themselves). The activities of the offices were not disrupted . . . . Nor was there any "inva[sion of] a person's private space," as in our hypothetical meter-reader case, as in the famous case of *De May v. Roberts* (1881) (where a doctor, called to the plaintiff's home to deliver her baby, brought along with him a friend who was curious to see a birth but was not a medical doctor, and represented the friend to be his medical assistant), as in one of its numerous modern counterparts, and as in *Dietemann v. Time, Inc.* (9th Cir. 1971), on which the plaintiffs in our case rely. *Dietemann* involved a home. True, the portion invaded was an office, where the plaintiff performed quack healing of nonexistent ailments. The parallel to this case is plain enough, but there is a difference. Dietemann was not in business, and did not advertise his services or charge for them. His quackery was private.

No embarrassingly intimate details of anybody's life were publicized in the present case. There was no eavesdropping on a private conversation; the testers recorded their own conversations with the Desnick Eye Center's physicians. There was no violation of the doctor-patient privilege. There was no theft, or intent to steal, trade secrets; no disruption of decorum, of peace and quiet; no noisy or distracting demonstrations. Had the testers been undercover FBI agents, there would have been no violation of the Fourth Amendment, because there would have been no invasion of a legally protected interest in property or privacy. "Testers" who pose as prospective home buyers in order to gather evidence of housing discrimination are not trespassers even if they are private persons not acting under color of law. The situation of the defendants' "testers" is analogous. Like testers seeking evidence of violation of anti-discrimination laws, the defendants' test patients gained entry into the plaintiffs' premises by misrepresenting their purposes (more precisely by a misleading omission to disclose those purposes). But the entry was not invasive in the sense of infringing the kind of interest of the plaintiffs that the law of trespass protects; it was not an interference with the ownership or possession of land. We need not consider what if any difference it would make if the plaintiffs had festooned the premises with signs forbidding the entry of testers or other snoops. Perhaps none, but that is an issue for another day.

The federal and state wiretapping statutes that the plaintiffs invoke allow one party to a conversation to record the conversation unless his purpose in doing so is to commit a crime or a tort or (in the case of the state, but not the federal, law) to do "other injurious acts." 18 U.S.C. § 2511(2)(d). The defendants did not order the camera-armed testers into the Desnick Eye Center's premises in order to commit a crime or tort.

Last is the charge of fraud in the defendants' gaining entry to the Chicago office . . . . The alleged fraud consists of a series of false promises by the defendants—that the broadcast segment would be fair and balanced and that the defendants would not use "ambush" interviews or undercover surveillance tactics in making the segment.

Unlike most states nowadays, Illinois does not provide a remedy for fraudulent promises ("promissory fraud")—unless they are part of a "scheme" to defraud. The distinction between a mere promissory fraud and a scheme of promissory fraud is elusive, and has caused, to say the

least, considerable uncertainty, as even the Illinois cases acknowledge. Some cases suggest that the exception has swallowed the rule. Others seem unwilling to apply the exception.

The distinction certainly is unsatisfactory, but it reflects an understandable ambivalence about allowing suits to be based on nothing more than an allegation of a fraudulent promise. There is a risk of turning every breach of contract suit into a fraud suit, of circumventing the limitation that the doctrine of consideration is supposed however ineptly to place on making all promises legally enforceable, and of thwarting the rule that denies the award of punitive damages for breach of contract. Our best interpretation is that promissory fraud is actionable only if it either is particularly egregious or, what may amount to the same thing, it is embedded in a larger pattern of deceptions or enticements that reasonably induces reliance and against which the law ought to provide a remedy.

We cannot view the fraud alleged in this case in that light. Investigative journalists well known for ruthlessness promise to wear kid gloves. They break their promise, as any person of normal sophistication would expect. If that is "fraud," it is the kind against which potential victims can easily arm themselves by maintaining a minimum of skepticism about journalistic goals and methods. Desnick, needless to say, was no tyro, or child, or otherwise a member of a vulnerable group. He is a successful professional and entrepreneur. No legal remedies to protect him from what happened are required, or by Illinois provided.

Notes

1. Desnick spent a great deal of time in court as a defendant for both these and other instances of misconduct, sued by many of his patients and ultimately settling claims of Medicare and Medicaid fraud for fourteen million dollars.
2. The investigators in *Desnick* told two different kinds of lies. The fake patients pretended to be real patients and the reporters pretended they were not engaged in a sting operation. For the fake patients, the example of the restaurant critic applies very well. But what about the reporters? Posner writes that Desnick should have expected them to break their promise. That is very different than how he defends the fake patients.
3. One useful framework for these kinds of cases focuses on the idea of special status. In some examples—such as Posner's restaurant critic or a customer conducting a secret audit—the individual withholds their identity to avoid special treatment. In others, an individual like a fake meter reader or a fraudulent employee assumes a special status that entitles them to privileged access they would not otherwise have received.

Council on American-Islamic Relations Action Network, Inc. v. Gaubatz, 793 F.Supp.2d 311 (D.D.C. 2011)

COLLEEN KOLLAR–KOTELLY, District Judge.

Plaintiffs Council on American–Islamic Relations Action Network, Inc. ("CAIR–AN") and CAIR–Foundation, Inc. ("CAIR–F") bring this action against two sets of defendants: Paul David Gaubatz and Chris Gaubatz (the "Gaubatz Defendants") and the Center for Security Policy, Inc. ("CSP") and three of its employees . . . . Plaintiffs allege that Defendants conceived and carried out a scheme to place Chris Gaubatz in an internship with CAIR–AN under an assumed identity, which allowed him to remove and copy thousands of Plaintiffs' internal documents and to record private conversations involving Plaintiffs' employees without consent or authorization. Plaintiffs contend that Defendants thereafter publicly disclosed and published the contents of those documents and recordings. In this action, Plaintiffs seek relief under Titles I and II of the Electronic Communications Privacy Act of 1986 (the "ECPA"), 18 U.S.C. §§ 2510–2712, and the common law of the District of Columbia.

CAIR–AN is a self-described national Muslim advocacy group with a mission that includes enhancing the understanding of Islam and promoting a positive image of Muslims in

the United States. CAIR–F is an organization supporting CAIR–AN and its mission. They share physical office space in the District of Columbia that is generally closed to the public and accessible to third parties only upon invitation.

Sometime prior to April 2008, Defendants conceived a plan to infiltrate Plaintiffs' offices with the aim of obtaining Plaintiffs' internal documents and recording conversations involving Plaintiffs' employees. According to their plan, Chris Gaubatz would attempt to secure an internship with CAIR–AN under an assumed identity and deliver any materials that he was able to obtain from Plaintiffs' offices to Paul David Gaubatz and the CSP Defendants for further dissemination.

Consistent with the agreed-upon plan, Chris Gaubatz sought and obtained an internship with the office for CAIR–AN Maryland/Virginia in April 2008. However, in June 2008, after it was announced that the office for CAIR–AN Maryland/Virginia would be closing, Chris Gaubatz sought an internship at CAIR–AN's headquarters in the District of Columbia.

Chris Gaubatz obtained his internship with CAIR–AN under false pretenses. During the application process, he made false statements and omitted important facts about his background, interests, and intentions. Among other things, he used an assumed name and represented that he was a student at a liberal arts college, that his father was in the construction business, and that he was a practicing Muslim. When Chris Gaubatz made these representations, he knew them to be false, and he made them in order to induce Plaintiffs to repose trust and confidence in him so that he might obtain an internship with CAIR–AN. He succeeded and was hired as an intern.

As a condition of and in consideration for his internship, Chris Gaubatz signed a confidentiality and non-disclosure agreement (the "Confidentiality Agreement"). Paul David Gaubatz and the CSP Defendants were aware of the Confidentiality Agreement . . . .

Chris Gaubatz worked as an intern for CAIR–AN until August 2008, though he returned to perform additional work over a weekend in September 2008. During the course of his internship, he sought to collect information about Plaintiffs and their employees with the intention of publicly disclosing that information for profit and in order to cast Plaintiffs in a negative light. To that end, he physically removed more than 12,000 of Plaintiffs' internal documents without authorization and delivered those documents to Paul David Gaubatz. Electronic documents, including e-mails and computer-generated spreadsheets, were obtained by accessing Plaintiffs' computers and computer systems with user-names and passwords that were not assigned to him.

Chris Gaubatz also used a concealed electronic device to make audio and video recordings of conversations involving Plaintiffs' employees without authorization and consent. He was able to compile over fifty computer discs containing recordings of Plaintiffs' employees. The Gaubatz Defendants delivered the recordings to CSP and Christine Brim who, with the assistance of the other CSP Defendants, organized and edited the recordings.

Defendants publicly disclosed the documents and recordings that they obtained from Plaintiffs. The CSP Defendants provided a compilation of recordings to the third-party publisher of WND Books and a website identified as WorldNet Daily. In addition, Paul David Gaubatz and a co-author wrote a book about Chris Gaubatz's internship with CAIR–AN. P. David Gaubatz & Paul Sperry, *Muslim Mafia: Inside the Secret World That's Conspiring to Islamize America* (1st ed., WND Books 2009) ("*Muslim Mafia*"). In *Muslim Mafia,* the authors characterize Chris Gaubatz's internship as a "six-month counterintelligence operation," admitting that Chris Gaubatz "routinely load[ed] the trunk of his car with boxes of sensitive documents and deliver[ed] them into the custody of investigative project leader P. David Gaubatz."

[Plaintiffs asserted a wide range of claims. Here we consider only two.]

Under District of Columbia law, a plaintiff asserting a claim for breach of fiduciary duty must allege that (i) the defendant had a fiduciary duty to the plaintiff, (ii) the defendant breached that duty, and (iii) the breach was the proximate cause of an injury.

Significantly, the District of Columbia courts have deliberately left the definition of a "fiduciary relationship" open-ended, allowing the concept to fit a wide array of factual circumstances. Deciding whether a fiduciary relationship exists in a particular case requires "a searching inquiry into the nature of the relationship, the promises made, the type of services or advice given and the legitimate expectations of the parties." Because the inquiry is fact-intensive, it is often inappropriate to decide whether a fiduciary relationship existed even in the context of a motion for summary judgment.

To the extent the Gaubatz Defendants intend to suggest that a fiduciary relationship can never exist between an intern and the entity engaging the intern, the aforementioned authorities foreclose such an expansive argument. Meanwhile, Plaintiffs allege that Chris Gaubatz secured his internship only by making a number of affirmatively false statements and omitting material information about his background, interests, and intentions with the specific intention of inducing Plaintiffs to repose a measure of trust and confidence in him, and that as a result of the trust and confidence reposed in him, Chris Gaubatz was afforded access to confidential, proprietary, and privileged materials as well as non-public areas of Plaintiffs' offices. These allegations imply a relationship akin to one between employer and employee, which under some circumstances may suffice to support a claim for breach of fiduciary duty under District of Columbia law. In any event, they suffice to suggest that the relationship between Chris Gaubatz and Plaintiffs extended beyond the normal bounds of a contractual relationship to form a special relationship founded upon trust and confidence. Whether Plaintiffs will be able to show that the relationship was grounded in a higher level of trust than is normally present between those involved in arm's-length business transactions is a question that must be answered after discovery.

Under District of Columbia law, a trespass is (i) an unauthorized entry (ii) onto the plaintiff's property (iii) that interferes with the plaintiff's possessory interest. In this case, Plaintiffs' trespass claim divides into two branches. First, Plaintiffs claim that Chris Gaubatz committed a trespass merely by entering their offices because he "only gained access to the property . . . through the use of pretense, subterfuge, misrepresentation, and/or concealment." Second, Plaintiffs claim that Chris Gaubatz committed a trespass by exceeding the consent he obtained from Plaintiffs by "stealing documents, accessing restricted areas and networks, and recording without permission conversations in Plaintiffs' offices." The Gaubatz Defendants present three reasons why they believe this claim should be dismissed.

First, the Gaubatz Defendants argue that Plaintiffs have failed to plead that "the premises were private and not open to the public." Even assuming that a plaintiff must plead that the property at issue was not open to the public in order to state a claim for trespass (something this Court doubts), Plaintiffs do allege that their offices "are not generally open to the public and may be accessed by third parties only upon invitation or authorization" and that "[t]he public is not permitted access to the areas of the offices . . . where documents are stored or maintained or where [Plaintiffs'] computers and computer servers, networks, and systems are stored and maintained." Given these express allegations, the Gaubatz Defendants' first argument is without merit.

Second, the Gaubatz Defendants argue that Plaintiffs' trespass claim must fail because they have not alleged damages. However, provided the damages are of the kind that would typically be expected to flow from a trespass, Plaintiffs are not required to plead their damages with particularity. Regardless, District of Columbia law allows a plaintiff to recover nominal damages for trespass. Therefore, even assuming for the sake of argument that Plaintiffs could not recover actual damages, that still would not be fatal to their claim.

Third, the Gaubatz Defendants argue that Plaintiffs' trespass claim must fail because Chris Gaubatz was authorized to enter Plaintiffs' offices. While this argument was first raised in reply, the Court will address it because Plaintiffs arguably opened the door in their opposition. However, the argument is unavailing. As an initial matter, it has no bearing on the second branch of Plaintiffs' trespass claim—namely, the contention that Chris Gaubatz exceeded the consent that he obtained from Plaintiffs by doing things like accessing restricted areas and networks. As a general matter, "[a] condition or restricted consent to enter land creates a privilege to do so only in so far as the condition or restriction is complied with." Restatement (Second) of Torts § 168 (1965). Therefore, "on-site employees may exceed the scope of their invitation to access, and so not be 'rightfully' on, the employer's property . . . at a place or time forbidden by their employer." *ITT Indus., Inc. v. Nat'l Labor Relations Bd.* (D.C. Cir. 2005).

As to the first branch of Plaintiffs' trespass claim—that is, the contention that Chris Gaubatz committed a trespass merely by entering Plaintiffs' offices because he obtained Plaintiffs' consent through subterfuge and fraud—the Gaubatz Defendants' consent argument is premature. Consent "given upon fraudulent misrepresentations" will not always defeat a claim for trespass. Consent may be ineffective if "induced . . . by a substantial mistake concerning the nature of the invasion of [the owner's] interests or the extent of the harm to be expected from it and the mistake is known to the other or is induced by the other's misrepresentation." Restatement (Second) of Torts §§ 173, 892B(2) (1965); *see also Desnick v. Am. Broad. Cos., Inc.* (7th Cir. 1995) (noting that it is no defense to trespass where "a competitor gain[s] entry to a business firm's premises posing as a customer but in fact hoping to steal the firm's trade secrets."). Because this is precisely what Plaintiffs have alleged occurred here, whether the Gaubatz Defendants' argument will win out is a question that must await discovery.

For the foregoing reasons, the Court will deny the Gaubatz Defendants' motion to dismiss insofar as it seeks dismissal of Plaintiffs' trespass claim. In summary, the Court will grant the motion insofar as it seeks dismissal of Plaintiffs' claim that Defendants converted Plaintiffs' electronic data and will deny the motion in all other respects.

Notes

1. The lies told by Chris Gaubatz were more extensive than those told in *Desnick*, but how clearly were they different *kinds* of lies? In each case, extra access was granted based on the affirmative misrepresentations of the person seeking to come in (the reporters in *Desnick*, not the fake patients). And, in each case, the lies were in service of reporting. Is the difference one of professionalism, such that we should be less accepting of the amateur reporting of CSP than the professional reporting of ABC, CNN, or Fox? Is the difference one of degree of access, whereby the reporters in *Desnick* got basic public relations access and the CSP agent instead stole thousands of files? Or are the lies themselves different, since being an employee carries with it a far greater degree of trust? Posner would presumably focus on the last of these.
2. In a similar case, reporters investigating the supermarket chain Food Lion submitted doctored resumes (misrepresenting names and educational histories, and also omitting current employment with ABC) and were hired by Food Lion. Among other things, they conducted videorecording in non-public areas. The reporters' story on Food Lion exposed unsafe and unsanitary meat handling practices that put public health at risk. The appellate court affirmed "the finding of trespass [by the reporters] on this ground because the breach of duty of loyalty—triggered by the filming in non-public areas, which was adverse to Food Lion—was a wrongful act in excess of Dale and Barnett's authority to enter Food Lion's premises as employees." *Food Lion, Inc. v. Cap. Cities/ABC, Inc.* 194 F.3d 505, 518 (4th Cir. 1999). Notably, the damages on the upheld trespass and breach of duty of loyalty claims amounted to only two dollars. The more substantial award for fraud was overturned on

causation grounds because the injuries suffered by Food Lion were not the result of the employees' misrepresentations but instead Food Lion's bad conduct.

B. Public disclosure of private facts

If intrusion upon seclusion is about inappropriately gathering information (or at least butting into things), public disclosure of private facts is about inappropriately sharing information. These torts are obviously complementary—it will often be the case that information is both inappropriately gathered and also inappropriately disclosed. But they are still distinct. One can intrude upon seclusion without disclosing and disclose without intruding upon seclusion.

One famous early public disclosure case was brought by a husband and wife whose photograph was taken at a farmers' market and then published in *Harper's Bazaar*, a major magazine with national circulation, and then subsequently in *Ladies' Home Journal*. The photo was used to accompany an article about everyday people in love. In dismissing the claim, the court stated, "In considering the nature of the picture in question, it is significant that it was not surreptitiously snapped on private grounds, but rather was taken of plaintiffs in a pose voluntarily assumed in a public market place. Here plaintiffs . . . had voluntarily exposed themselves to public gaze in a pose open to the view of any persons who might then be at or near their place of business. By their own voluntary action plaintiffs waived their right of privacy so far as this particular public pose was assumed, for 'There can be no privacy in that which is already public.'" *Gill v. Hearst Pub. Co.* 253 P.2d 441 (Cal. 1953). The photo was also not anything "beyond the limits of decency."

This is consistent with the general theme of subsequent cases. Much happens in public, and what happens in public is not private. There are rare exceptions to this rule. In *Daily Times Democrat v. Graham* 162 So. 2d 474 (Ala. 1964), a housewife was able to sustain a privacy suit against a newspaper that published a photo of her with her dress blown up above her waist by an air vent at a funhouse. Though the photo was taken in public, "[t]o hold that one who is involuntarily and instantaneously enmeshed in an embarrassing pose forfeits her right of privacy merely because she happened at the moment to be part of a public scene would be illogical, wrong, and unjust."

1) Elements of public disclosure

Finley v. Kelly, 384 F.Supp.3d 898 (M.D. Tenn. 2019)

WAVERLY D. CRENSHAW, JR. CHIEF UNITED STATES DISTRICT JUDGE,

In this diversity action brought by Roger and Kerry Finley, Robyn Kelly has filed a Motion to Dismiss . . . . [AUTH: The court uses first names to avoid confusion.]

Eliminating some of the legal conclusions (of which there are many), and toning down the hyperbole a tad, the Amended Complaint alleges the following relevant facts:

Robyn and Roger dated in high school and had a brief romantic relationship. Decades later, they reconnected on Facebook and arranged a meeting in Las Vegas. Robyn and her husband . . . met Roger there in January 2013. The trio met again in Las Vegas in January 2014.

After the January 2014 meeting, Robyn and Roger never met again. They did, however, correspond for several months in 2014, and discussed rekindling their decades-old high school relationship. By September 2014, however, Roger decided that it was wrong for him to engage

in such communications, and he informed Robyn that he did not wish to communicate with her further. This did not go over well.

In December of 2014, Robyn, utilizing a fake Facebook account, began sharing personal messages with Kerry [Roger's wife] that she had received from Roger. This prompted Kerry to block Robyn on Facebook. Thwarted, Robyn changed tactics by "leaving lengthy voicemails and sending literally hundreds of emails to Roger," that included "threats of public disclosure of private facts" and "contained vitriolic attacks on Roger and vicious and frightening attacks on his wife, Kerry."

Roger, too, was forced to shut down his personal Facebook account, but could not change his work email. He tried to block messages from Robyn, but she would circumvent this by creating a "myriad [of] new email accounts," through which she sent "messages several times per week to his work email system from late 2014 into the late spring or 2018." Some emails threatened to get Roger fired from his job . . . .

Robyn routinely threatened to "'expose' Roger to a 'larger audience' and made other clear threats that she would inform third parties of her 'beliefs' about Roger—*i.e.*, the . . . false assertions that Roger is an abusive romantic partner and a belligerent alcoholic, and his wife Kerry has physically threatened her—and provide those individuals with copies of the messages sent privately by Roger to Robyn." Robyn made good on those threats when, utilizing the "handle Grace Squad," she created a Facebook account and uploaded a 79-page "Document" that included private exchanges and photos between her and Roger. The Document was prefaced with an introductory 15-page, single spaced narrative that contained many of the same "salacious" claims, "accusations," and "vitriolic attacks" she had unleashed before in her private communications with Roger and Kerry. The Document was sent to at least 18 individuals, some of whom were Plaintiffs' family members and personal friends.

In addition to repeating a lot of what had been said earlier, the narrative portion of the Document "describes Roger as "a psycho and pathological liar," "obsessive," "an abuser," and a "stalker" who purportedly "mistreated" and "threatened Robyn." The Document also states that Roger was "a drunk," "mentally unhealthy," and that a psychologist friend of Robyn's indicated that Roger's behavior "fit every definition and description of a sociopath." The Document also attacks Kerry, claiming that the Finleys had "an abusive relationship," and that Kerry was belligerent, threatening and "abus[ive] to Roger." The Document continues in the same vein, but this is more than enough to describe its essence and place the parties' arguments in context.

Based primarily upon the Document, Roger and Kerry bring state causes of action for defamation (Count One); invasion of privacy via the public disclosure of private facts (Count Two) and intrusion upon seclusion (Count Three) . . . .

Public Disclosure of Private Facts

[W]hile "[t]he Tennessee Supreme Court has not expressly recognized the public disclosure of private facts form of invasion of privacy," "Tennessee courts of appeal have recognized this tort." What the cases also show, however, is that most are dismissed because "[e]ssential to sustaining this cause of action is a showing of a *public* disclosure of private facts," and "[c]ommunication to a single individual or to a small group of people, absent breach of contract, trust or other confidential relationship will not give rise to liability."

Here, in moving to dismiss on the familiar ground that the allegedly defamatory statements were insufficiently published, Robyn acknowledges that "the case law does not provide a 'magic number' of recipients that must receive a message for it to be considered 'public' disclosure[.]" She points out, however, that "[s]ix to eight" people was found to be insufficient and speculates that because the insufficient disclosure in *Garmley v. Opryland Hotel Nashville, LLC* (M.D. Tenn. 2007) was to a "corporate employer . . . the information may have been received

by many more than [the] eighteen people" that are alleged to have received the Document in this case.

Even though Tennessee courts appear not to have addressed the issue, a number of courts when considering the tort of public disclosure of private facts have endorsed an exception that holds that the publicity element may be satisfied where the information is released to a small number of persons who have a special relationship with the plaintiff, such as family members. Others have not. Still others have failed to take a position one way or the other.

If Tennessee courts were to adopt this exception, then Plaintiffs easily state a plausible claim. They allege that the Document was provided to their relatives and friends, which, at least arguably, "makes the disclosure as devastating as disclosing the information to the public at large." Fortunately, however, the Court need not divine what the Tennessee courts might do because, even if publication must be broader, plaintiffs have alleged a *plausible* allegation that the allegedly defamatory statements were further distributed. Though professing "not . . . to make this a #metoo revelation," Robyn states in the Document that, "my husband and I have shared this story and information with family and friends." Moreover, because the Document was shared in digital format, it would not take much to resend the Document to others. Only discovery can sort out this issue. Plaintiffs' public disclosure of private facts claim will not be dismissed.

Intrusion upon Seclusion

Just as with the tort of public disclosure of private facts, the Tennessee Supreme Court has yet to recognize intrusion upon seclusion as a separate cause of action for invasion of privacy, but the Tennessee Court of Appeals has and "the scope of this tort is parallel to that contained in section 652B of the Restatement (Second) of Torts." Under the Restatement, "the defendant is subject to liability . . . only when he has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs." This "requires the plaintiff to plead and prove three elements: (1) an intentional intrusion, physical or otherwise; (2) upon the plaintiff's solitude or seclusion or private affairs or concerns; (3) which would be highly offensive to a reasonable person." "The essential question to be answered with respect to this issue, then, is whether the complaint has pled facts showing that [defendant] 'invaded a private seclusion that the plaintiff[s have] thrown about [their] persons or affairs." Here, that question must be answered in the negative.

"[T]he finding of an intrusion is tied to the plaintiff's expectation of privacy," and "in order to prove that there has been an intentional intrusion into a private place, conversation or matter, the plaintiff will usually have to prove that there was: (1) an actual, subjective expectation of seclusion or solitude in that place, conversation or matter; and that (2) that expectation of privacy was objectively reasonable." Thus, for example, "opening plaintiff's private mail and reading it without authority" is an intrusion into privacy, but plaintiff does not have a reasonable expectation of privacy in what she throws into the trash even if she "had a subjective expectation that her trash would remain private." Likewise, "hacking into a person's private computer and stealing personal correspondence [represents] an intentional intrusion on the victim's private affairs," but a plaintiff does not have "a reasonable expectation of privacy in words he had already conveyed to a third party that the third party then decided to disclose."

"The maxim of law that one 'who consents to an act is not wronged by it' applies to the tort of invasion of privacy," and "[t]he right of privacy may be waived or lost by consent." Here, Roger may have subjectively believed that he and Robyn had reached some sort of understanding regarding their exchange of communications via email and messaging, but when he hit the send button he lifted the cloak "thrown about his person or affairs" in relation to those messages and placed his fate in Robyn's hands. Accordingly, Plaintiffs' intrusion into seclusion claim will be dismissed.

Notes

1. As is so often true in these cases, both defamation and public disclosure of private facts are at issue. Public disclosure is for true claims, defamation for false ones, and discovery for telling the difference. As will be seen below, defamation requires something to be a statement of fact. Here, the defendant argued that her many statements about the plaintiffs were instead mere opinion. The court rejected this: "[W]hile calling someone a monster or a creep may not be defamatory because it is hyperbole or an expression of opinion, referring to someone as a stalker can be" because it attributes criminal activity to the person. Similarly, referring to someone as a sociopath, alcoholic, or drunk may be defamatory; whether that counts as a sufficiently factual claim can be a jury question.

In re Facebook, Inc., Consumer Privacy User Profile Litig., 402 F.Supp.3d 767 (N.D. Cal. 2019)

VINCE CHHABRIA, United States District Judge

This lawsuit, which stems from the Cambridge Analytica scandal, is about Facebook's practice of sharing its users' personal information with third parties. The plaintiffs are current and former Facebook users who believe that their information was compromised by the company. Their principal allegations are that Facebook: (i) made sensitive user information available to countless companies and individuals without the consent of the users; and (ii) failed to prevent those same companies and individuals from selling or otherwise misusing the information. The plaintiffs do not merely allege that Facebook shared what we often describe as "data"—basic facts such as gender, age, address, and the like. They allege that Facebook shared far more substantive and revealing content that users intended only for a limited audience, such as their photographs, videos they made, videos they watched, their religious and political views, their relationship information, and the actual words contained in their messages.

I. BACKGROUND

Cambridge Analytica, a British political consulting firm, used personal information from millions of Facebook accounts to send targeted political messages during the 2016 presidential campaign. The firm obtained this information from Aleksandr Kogan, a researcher who had acquired it through his app, which Facebook had allowed him to deploy on its platform. The Cambridge Analytica incident began receiving significant press coverage in 2018, which in turn generated increased scrutiny of Facebook's information-sharing practices.

The core allegations in the complaint describe four categories of wrongdoing by Facebook. In adjudicating Facebook's motion to dismiss, the Court is required to assume the truth of these allegations, so long as they are adequately articulated and not contradicted by any documents that the complaint explicitly relies on.

1. Giving app developers access to sensitive user information. Since roughly 2007, Facebook users have been able to access applications, or apps, directly from the Facebook platform to do things like play video games, read news content, or stream videos. According to the plaintiffs, this interaction among Facebook, its users, and third-party apps is one of the primary means by which Facebook has disseminated user information to third parties. The complaint alleges that when users accessed apps on the Facebook platform, the app developers were not merely able to obtain information about the users they were interacting with; they were also able to obtain any information about the users' Facebook friends that the users themselves had access to. So, for example, if you decided to use an app on the Facebook platform to play a video game, the video game company would be able to access not only your information but also any information about your friends that you could obtain yourself. This includes a variety of things that your friends might have intended to share only with a limited audience,

such as photographs, videos they made, videos they watched, religious preferences, posts, and even sometimes private one-on-one messages sent through Facebook. And since most people have dozens or hundreds of Facebook friends, each interaction with an app represents the disclosure of a great deal of information about dozens or hundreds of people.

2. Continued disclosure to whitelisted apps. In 2014, in response to criticism of its information-sharing practices, Facebook announced it would restrict app developers so they would have access only to the information of the users the apps were interacting with (and not to information of the users' friends). But the plaintiffs allege that Facebook, despite its public promises to restrict access, continued to allow a preferred list of app developers to access the information of users' friends. The complaint describes these preferred app developers as "whitelisted apps," and alleges that Facebook secretly continued to give these apps "special access" to friends' information because of the amount of revenue these apps generated for Facebook. Thousands of companies were allegedly on this list, including Airbnb, Netflix, UPS, Hot or Not, Salesforce, Lyft, Telescope, and Spotify.

3. Sharing sensitive user information with business partners. Meanwhile, Facebook has maintained a separate information-sharing program with companies that the plaintiffs describe as "business partners." The complaint's allegations about these business partners are somewhat more difficult to pin down than the allegations about app developers. Indeed, there may be some overlap between companies in the "app" category and the "business partner" category. Moreover, the plaintiffs allege that Facebook outsourced to business partners "the time, labor, and money required to build Facebook's Platform on different devices and operating systems," but that doesn't seem to describe all the "business partners" listed in the complaint.

Although the category is somewhat vague, the alleged misconduct is relatively straightforward. The complaint alleges that Facebook shared information about its users with this non-exclusive list of business partners, and that those companies in turn shared data with Facebook. "These partnerships," the complaint alleges, "were built in part on 'data reciprocity.'"

4. Failure to restrict the use of sensitive information. In addition to complaining about Facebook's dissemination of private user information to app developers, whitelisted apps, and business partners, the plaintiffs allege that Facebook did nothing to prevent these third parties from misusing the information Facebook allowed them to access.

Again, the Cambridge Analytica story is an example of this. According to the plaintiffs, if Facebook was truly enforcing a policy of limiting the use of user information by app developers, Kogan would have been precluded from extracting all that sensitive information about users' friends to employ for his own research, and he would certainly have been precluded from selling it to Cambridge Analytica. The plaintiffs allege that this was the norm with the tens of thousands of app developers who interacted with users on the Facebook platform—that any policy Facebook purported to have restricting the use of information by third parties was nonexistent in reality, because Facebook was intent solely on generating revenue from the access it was providing.

II. EXPECTATION OF PRIVACY

Facebook's motion to dismiss is littered with assumptions about the degree to which social media users can reasonably expect their personal information and communications to remain private. Because Facebook's view of this issue pervades so many of its individual legal arguments—and because Facebook's view is so wrong—it is addressed at the outset.

Facebook's view is that once you make information available to your friends on social media, you completely relinquish any privacy interest in that information. For this reason, Facebook insists, it does not matter whether Facebook users consented to the company's information-sharing practices. Facebook asserts that even if users didn't consent, and even if users intended to restrict access to friends only, and even if Facebook had explicitly promised

not to share their information with anyone else, the users would have no right to complain that their privacy was invaded by the disclosure or misuse of their sensitive information.

The problem with Facebook's argument is that it treats privacy as an all-or-nothing proposition—either you retain a full privacy interest by not sharing information with anyone, or you have no privacy interest whatsoever by virtue of sharing it even in a limited fashion. In reality, there can be "degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law." Thus, as the U.S. Supreme Court has explained, "information may be classified as private if it is intended for or restricted to the use of a particular person *or group or class of persons*" rather than being "freely available to the public." *U.S. Department of Justice v. Reporters Committee for Freedom of the Press* (1989) (emphasis added). So, for example, if you are diagnosed with a medical condition, you can expect to conceal it completely only if you keep it between you and your doctor. But it does not follow that if you send an email to selected colleagues and friends explaining why you'll be out of commission for a while, you've relinquished any privacy interest in your medical condition, such that the email provider could disseminate your diagnosis to anyone who might be interested in your health status. Similarly, social media users can have their privacy invaded if sensitive information meant only for a few dozen friends is shared more widely.

Although Facebook refuses in this case to acknowledge its users' privacy interests, it has done so in other court cases. For example, in a brief filed with the California Supreme Court, for a case where Facebook fought against the compelled disclosure of a user's posts, Facebook compared information kept on social media to information kept on a smartphone: "The data on a smartphone— like the data maintained in a social media account— can reveal an individual's private interests and concerns and where a person has been, which in turn reflects a wealth of detail about a person's familial, political, professional, religious, and sexual associations." For this reason, Facebook continued, "communications content of the kind maintained by [social media] providers" carries with it such a significant expectation of privacy that even law enforcement must get a warrant before accessing it from those providers. In a different California Supreme Court brief, Facebook took pains to juxtapose users who share communications with the general public against users who share communications only with friends: "These settings cannot be overridden by others; if a post is set to be viewable only by a certain audience, it may not then be shared or forwarded through the Facebook platform to someone outside that audience." Facebook added that even if users designate their communications to be viewed by the general public, they can later "regain" their expectation of privacy in that information by switching their settings back to a more restricted audience.

Perhaps Facebook's argument that social media accounts are like smartphones is an exaggeration in the other direction. But it's closer to the truth than the company's assertions in this case. Sharing information with your social media friends does not categorically eliminate your privacy interest in that information, and the plaintiffs' claims in this lawsuit must be analyzed against that backdrop, rather than the backdrop Facebook attempts to paint in its motion to dismiss.

IV. CONSENT

Facebook contends that the plaintiffs agreed, when they signed up for their accounts, that Facebook could disseminate their "friends only" information in the way it has done.

[T]he parties agree that California law requires the Court to pretend that users actually read Facebook's contractual language before clicking their acceptance, even though we all know virtually none of them did. Constrained by this fiction, the Court must analyze the relevant contractual language to assess whether the users "agreed" to allow Facebook to disseminate their sensitive information in the ways described in the lawsuit. The upshot, at this early stage of the case, is that if a reasonable Facebook user could plausibly have interpreted the contract

language as *not* disclosing that Facebook would engage in particular conduct, then Facebook cannot obtain dismissal of a claim about that conduct (at least not based on the issue of consent).

One difficulty with the consent question is that the lawsuit covers a nearly 13-year period—from 2007 to the present. Obviously, Facebook said different things to its users over that period, and its practices changed as well. The analysis in this ruling will primarily focus on the documents presented to users who signed up for accounts in the middle of 2012.

People who signed up for accounts in mid-2012 were required to accept Facebook's "Statement of Rights and Responsibilities," or "SRR." The SRR itself contains some statements about privacy and information-sharing. But it also references, and contains links to, several other policies, including the "Data Use Policy."

The first section of the SRR, entitled "Privacy," calls out the Data Use Policy in the second sentence, provides a link to it, and encourages the user to read it. This first section of the SRR states in full: "Your privacy is very important to us. We designed our Data Use Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Use Policy, and to use it to help you make informed decisions." Later on the same page, the SRR tells users to read the Data Use Policy to learn about "how you can control what information other people may share with applications." And at the end, the SRR provides a list of additional documents the user "may also want to review," including the Data Use Policy, which "contains information to help you understand how we collect and use information." This final section again includes a link to the Data Use Policy . . . .

This is sufficient to incorporate the Data Use Policy into the contractual agreement between Facebook and its users. Thus, the true legal question is whether, by "agreeing" to the SRR and Data Use Policy, Facebook users consented to the alleged misconduct. In analyzing this question, it's important to reiterate the precise conduct at issue. Recall that the plaintiffs allege four categories of misconduct: (i) Facebook allowed app developers to access sensitive information, not merely of users they interacted with, but of the users' friends; (ii) even after Facebook announced it would no longer give app developers access to information of users' friends, it secretly continued to give "whitelisted apps" access; (iii) through some separate arrangement and by some separate means, Facebook shared sensitive user information with its business partners; and (iv) although Facebook ostensibly had a policy of sharply limiting the use of the sensitive information it gave to third parties, in fact Facebook imposed no limits whatsoever.

It's easy to conclude, at the pleading stage, that the second category of conduct was not disclosed. In fact, Facebook does not even argue that its users assented to this practice. The same goes for the third category: although Facebook points to a section in its Data Use Policy entitled "Service Providers" which says "we give your information to the people and companies that help us provide, understand, and improve the services we offer," that statement does not come close to disclosing the massive information-sharing program with business partners that the plaintiffs allege in the complaint.

In contrast, the first category of conduct—allowing the Aleksandr Kogans of the world to interact with users and obtain information of the users' friends through those interactions—was disclosed in the terms agreed to by Facebook users, at least for a portion of the period covered by this lawsuit. As mentioned previously, the SRR also flagged for users the possibility that other people "may share" their information "with applications," and instructed users to read the Data Use Policy to learn more about this. In turn, the Data Use Policy said that "if you share something on Facebook anyone who can see it can share it with others, including the games, applications, and websites they use." And it instructed: "If you want to completely block applications from getting your information when your friends and others use them, you will

need to turn off all Platform applications. This means you will no longer be able to use any third-party Facebook-integrated games, applications, or websites."

To be sure, for the rare person who actually read the contractual language, it would have been difficult to isolate and understand the pertinent language among all of Facebook's complicated disclosures. Thus, in reality, virtually no one "consented" in a layperson's sense to Facebook's dissemination of this information to app developers. But under California law, users must be deemed to have agreed to the language quoted in the preceding paragraph, which means that users who did not properly adjust their application settings are deemed to have agreed that app developers could access their information.

But there is a caveat. One inference from the complaint and the judicially noticeable materials is that Facebook began to disclose this practice of giving app developers access to friends' information only around 2009. Thus, users who established Facebook accounts before this time did not, at least based on the allegations in the complaint, agree to these terms when they signed up. Facebook contends this does not matter, because those users agreed to be bound by the SRR and Data Use Policy going forward, even when the terms changed. There appears to be some disagreement in the courts about whether a unilateral modification provision of this sort is permissible under California contract law, at least in circumstances where the party against whom it is being asserted did not receive adequate notice of the modification.

The fourth category of alleged misconduct—failing to limit how third parties could use the sensitive information they accessed—is also somewhat complicated. The Data Use Policy, after explaining to users that applications could obtain their information from their friends, stated as follows: "If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission and no one else." The Policy gives an example of this: "one of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list—which includes your User ID—so the application knows which of her friends is also using it." From this example, it seems clear that the phrase "the application will be allowed to use that information only in connection with the person that gave the permission" means that if an app developer accesses your information through interaction with one of your Facebook friends, it may use your information only as part of its interaction with that friend. It therefore may not sell your information, or use it to develop a digital dossier on you for future targeted advertising.

Less clear is what Facebook is promising to do to protect users. Facebook interprets the disclosure to mean, in essence, "we tell app developers that they can only use your information to facilitate their interactions with your friends, but you can't really be sure they'll honor that." Perhaps a reasonable Facebook user could interpret the disclosure that way, which would mean that the user, upon agreeing to the Data Use Policy, assumed the risk that app developers would misuse the information. In other words, on this interpretation, users consented to an arrangement whereby app developers could end up obtaining their sensitive information for any purpose. But recall that in the context of this motion to dismiss the plaintiffs may be deemed to have consented to this arrangement only if that is the only plausible interpretation. It is not—there are at least two others. One equally plausible interpretation of the disclosure is that it assures users that Facebook is actively policing the activities of app developers on its platform, and thereby successfully preventing sensitive information from being misappropriated. Another plausible interpretation is that the word "allowed" references a technological block of sorts—that is, perhaps a user could conclude that the Facebook platform has the ability to physically prevent app developers from being able to "see" friend information outside the context of their interactions with users. A user who has tried to access a fantasy football website at work, only to see a message on his screen that he's not "allowed" to access the site from that computer, might interpret the disclosure this way. Indeed, the Data Use

Policy elsewhere uses the word "allowed" in a similar fashion, to connote a technological block. For example, it states: "If someone clicks on a link to another person's timeline, they'll only see the things that they are allowed to see." Thus, there are at least three plausible interpretations of the contract language, two of which would lead to a conclusion that users did not consent but were misled, because Facebook allegedly did nothing to enforce its purported policy against tens of thousands of app developers who were freely making off with sensitive user information.

The bottom line on the issue of consent is this: the complaint plausibly alleges that some users (and some plaintiffs) did not consent to the arrangement whereby app developers could access their sensitive information simply by interacting with their friends. For the remaining three categories of misconduct—sharing with whitelisted apps, sharing with business partners, and failing to prevent misuse of information by third parties—the complaint plausibly alleges that none of the users consented. The issue of consent therefore does not require dismissal in full of any of the prioritized claims in this lawsuit.

V. INDIVIDUAL CLAIMS

Public disclosure of private facts. For this tort to give rise to liability, the following must occur: (i) the defendant must disclose a private fact about the plaintiff; (ii) the private fact must not be a matter of public concern; (iii) the disclosure must be to the public; and (iv) the disclosure must be offensive and objectionable to a reasonable person. *See Doe v. Gangland Productions., Inc.* (9th Cir. 2013). The plaintiffs have adequately alleged that Facebook engaged in this conduct.

Facebook argues that the information about users that it disclosed to app developers was not "private" because users had allowed their Facebook friends to access that information. But as discussed in Section II, your sensitive information does not lose the label "private" simply because your friends know about it. Your privacy interest in that information may diminish because you've shared it with your friends, but it does not necessarily disappear. For example, the plaintiffs allege that app developers accessed information about their religious preferences and political views. Your friends may know about your religious and political views, but the widespread dissemination of them can still invade your privacy. The plaintiffs also allege that some of the information app developers received would allow them to discern a user's location (for example, a post saying "Check out where I'm staying in June!"). If you've told your friends where you'll be at a particular time, that does not preclude a lawsuit based on the widespread, nonconsensual distribution of that information.

Facebook also argues that the user information was not disseminated to "the public." [D]issemination of your private information to tens of thousands of individuals and companies is generally going to be equivalent to making that information "public." Perhaps Facebook could have made a better argument, which is that there's a difference between publicizing your sensitive information for actual human beings to scrutinize (like, in a newspaper) and allowing your information to be added to the vast sea of "big data" that computers rather than humans analyze for the purpose of sending targeted advertising on behalf of companies. Perhaps there is an argument that the former is the "public disclosure" of information within the meaning of California law while the latter is not. But that is not an issue that can be resolved at this stage of the litigation: Facebook does not pursue this argument, and in any event the plaintiffs do not allege that their information was merely subject to relatively anonymous computer analysis.

Finally, Facebook contends that its disclosure of sensitive user information to app developers and business partners would not be offensive to a reasonable person. "Sharing is the social norm undergirding Facebook," the company argues, "and Facebook did not breach that social norm by sharing user data consistent with users' preferences." There are a number of problems with this assertion. First, it again erroneously assumes a "norm" that there is no privacy interest in the information kept on social media. The social norm Facebook created with its product is purposefully sharing with one's friends, not having one's information shared by

Facebook with unknown companies and individuals. Second, it assumes that users consented to the widespread disclosure of their sensitive information, but the plaintiffs have adequately alleged that they didn't. Thus, at this stage of the case, the plaintiffs have adequately alleged that Facebook's conduct was offensive and an egregious breach of social norms: it disclosed to tens of thousands of app developers and business partners sensitive information about them without their consent, including their photos, religious preferences, video-watching habits, relationships, and information that could reveal location. It even allegedly disclosed the contents of communications between two people on Facebook's ostensibly private messenger system.

The motion to dismiss this claim is granted with respect to the first category of conduct for plaintiffs who consented to this conduct, as discussed in Section IV. It is denied in all other respects.

Intrusion on private affairs and violation of the constitutional right to privacy. The analysis for these two tort claims is functionally identical, even though each claim is described somewhat differently in the case law. "When both claims are present, courts conduct a combined inquiry that considers (1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification or other relevant interests." Under California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is. *Williams v. Facebook, Inc.* (N.D. Cal. 2018) (Whether conduct rises to the level of highly offensive "is indeed a factual question best left for a jury."); *Opperman v. Path, Inc.* (N.D. Cal. 2016) ("A judge should be cautious before substituting his or her judgment for that of the community."). For the reasons already discussed, the plaintiffs have adequately alleged that they suffered an egregious invasion of their privacy when Facebook gave app developers and business partners their sensitive information on a widespread basis.

The motion to dismiss this claim is granted with respect to the first category of conduct for plaintiffs who consented to this conduct, as discussed in Section IV. It is denied in all other respects.

Right of Publicity. California's common law right of publicity makes unlawful the appropriation of someone's name or likeness without his consent when it both (1) injures that person and (2) is used to the defendant's advantage.

Facebook's motion to dismiss this claim is granted. The allegations about how Facebook shared the plaintiffs' information with third parties is categorically different from the type of conduct made unlawful by this tort, such as using a plaintiff's face or name to promote a product or service. Because the Court cannot conceive of a way that the plaintiffs could successfully allege this claim, dismissal is without leave to amend.

Notes

1. There is quite a lot going on here. It is helpful to break this opinion down into two basic questions. First, is information posted to Facebook and shared with only Facebook friends ever "private" for the purposes of tort law? Second, is Facebook's collection of user agreements sufficient to give it consent to do the various things it did? For the first question, the court gives a clear "yes." Does that strike you as correct? Imagine if your friend posts to their 300 friends that they support the British Labour Party. Is that a private fact?
2. The collection of user agreements shows how messy major litigation can be in this context. Companies put out dozens of related policies that may amount to hundreds of pages of text. The court here correctly concludes that it is bound to consider all of them even though it is fully aware that few, if any, customers actually read the documents in their entirety. What do we make of its analysis? Some of those disclosures are quite clear and are used to toss

claims (for those users who definitively assented to them). Is it fair to the users to hold them to these agreements? Is it fair to the companies to not hold users to them?

3. Sometimes students look at the kinds of cases in this chapter and have difficulty seeing the connection between the individual grievances litigated here and the large-scale corporate work that may await them after graduation. This case is here, in part, to show the linkage. The same causes of action used between former friends, lovers, and colleagues are sometimes also used against multinational corporations.

2) Newsworthiness

Shulman v. Group W Productions, Inc., 955 P.2d 469 (Cal. 1998)

WERDEGAR, Justice.

In the present case, we address the balance between privacy and press freedom in the commonplace context of an automobile accident.

On June 24, 1990, plaintiffs Ruth and Wayne Shulman, mother and son, were injured when the car in which they and two other family members were riding on interstate 10 in Riverside County flew off the highway and tumbled down an embankment into a drainage ditch on state-owned property, coming to rest upside down. Ruth, the most seriously injured of the two, was pinned under the car. Ruth and Wayne both had to be cut free from the vehicle by the device known as "the jaws of life."

A rescue helicopter operated by Mercy Air was dispatched to the scene. The flight nurse, who would perform the medical care at the scene and on the way to the hospital, was Laura Carnahan. Also on board were the pilot, a medic and Joel Cooke, a video camera operator employed by defendants Group W Productions, Inc., and 4MN Productions. Cooke was recording the rescue operation for later broadcast.

Cooke roamed the accident scene, videotaping the rescue. Nurse Carnahan wore a wireless microphone that picked up her conversations with both Ruth and the other rescue personnel. Cooke's tape was edited into a piece approximately nine minutes long, which, with the addition of narrative voice-over, was broadcast on September 29, 1990, as a segment of *On Scene: Emergency Response*.

The segment begins with the Mercy Air helicopter shown on its way to the accident site. The narrator's voice is heard in the background, setting the scene and describing in general terms what has happened. The pilot can be heard speaking with rescue workers on the ground in order to prepare for his landing. After Carnahan steps from the helicopter, she can be seen and heard speaking about the situation with various rescue workers. A firefighter assures her they will hose down the area to prevent any fire from the wrecked car.

The videotape shows only a glimpse of Wayne, and his voice is never heard. Ruth is shown several times, either by brief shots of a limb or her torso, or with her features blocked by others or obscured by an oxygen mask. She is also heard speaking several times. Carnahan calls her "Ruth" and her last name is not mentioned on the broadcast.

While Ruth is still trapped under the car, Carnahan asks Ruth's age. Ruth responds, "I'm old." On further questioning, Ruth reveals she is 47, and Carnahan observes that "it's all relative. You're not that old." During her extrication from the car, Ruth asks at least twice if she is dreaming. At one point she asks Carnahan, who has told her she will be taken to the hospital in a helicopter: "Are you teasing?" At another point she says: "This is terrible. Am I dreaming?" She also asks what happened and where the rest of her family is, repeating the questions even after being told she was in an accident and the other family members are being cared for. While being loaded into the helicopter on a stretcher, Ruth says: "I just want to die."

Carnahan reassures her that she is "going to do real well," but Ruth repeats: "I just want to die. I don't want to go through this."

Ruth and Wayne are placed in the helicopter, and its door is closed. The narrator states: "Once airborne, Laura and [the flight medic] will update their patients' vital signs and establish communications with the waiting trauma teams at Loma Linda." Carnahan, speaking into what appears to be a radio microphone, transmits some of Ruth's vital signs and states that Ruth cannot move her feet and has no sensation. The video footage during the helicopter ride includes a few seconds of Ruth's face, covered by an oxygen mask. Wayne is neither shown nor heard.

The helicopter lands on the hospital roof. With the door open, Ruth states while being taken out: "My upper back hurts." Carnahan replies: "Your upper back hurts." That's what you were saying up there." Ruth states: "I don't feel that great." Carnahan responds: "You probably don't."

Finally, Ruth is shown being moved from the helicopter into the hospital. The narrator concludes by stating: "Once inside both patients will be further evaluated and moved into emergency surgery if need be. Thanks to the efforts of the crew of Mercy Air, the firefighters, medics and police who responded, patients' lives were saved." As the segment ends, a brief, written epilogue appears on the screen, stating: "Laura's patient spent months in the hospital. She suffered severe back injuries. The others were all released much sooner."

The accident left Ruth a paraplegic. When the segment was broadcast, Wayne phoned Ruth in her hospital room and told her to turn on the television because "Channel 4 is showing our accident now." Shortly afterward, several hospital workers came into the room to mention that a videotaped segment of her accident was being shown. Ruth was "shocked, so to speak, that this would be run and I would be exploited, have my privacy invaded, which is what I felt had happened." She did not know her rescue had been recorded in this manner and had never consented to the recording or broadcast. Ruth had the impression from the broadcast "that I was kind of talking non-stop, and I remember hearing some of the things I said, which were not very pleasant." Asked at deposition what part of the broadcast material she considered private, Ruth explained: "I think the whole scene was pretty private. It was pretty gruesome, the parts that I saw, my knee sticking out of the car. I certainly did not look my best, and I don't feel it's for the public to see. I was not at my best in what I was thinking and what I was saying and what was being shown, and it's not for the public to see this trauma that I was going through."

Ruth and Wayne sued the producers of *On Scene: Emergency Response,* as well as others. The first amended complaint included two causes of action for invasion of privacy, one based on defendants' unlawful intrusion by videotaping the rescue in the first instance and the other based on the public disclosure of private facts, i.e., the broadcast.

I. Publication of Private Facts

The claim that a publication has given unwanted publicity to allegedly private aspects of a person's life is one of the more commonly litigated and well-defined areas of privacy law**.** [T]he following elements of the public disclosure tort [are]: "(1) public disclosure (2) of a private fact (3) which would be offensive and objectionable to the reasonable person and (4) which is not of legitimate public concern."

The element critical to this case is the presence or absence of legitimate public interest, i.e., newsworthiness, in the facts disclosed. Newsworthiness—constitutional or common law—is also difficult to define because it may be used as either a descriptive or a normative term. "Is the term 'newsworthy' a descriptive predicate, intended to refer to the fact there is widespread public interest? Or is it a value predicate, intended to indicate that the publication is a meritorious contribution and that the public's interest is praiseworthy?"

Our prior decisions have not explicitly addressed the type of privacy invasion alleged in this case: the broadcast of embarrassing pictures and speech of a person who, while generally

not a public figure, has become involuntarily involved in an event or activity of legitimate public concern. We nonetheless draw guidance from those decisions, in that they articulate the competing interests to be balanced. First, the analysis of newsworthiness does involve courts to some degree in a normative assessment of the "social value" of a publication. All material that might attract readers or viewers is not, simply by virtue of its attractiveness, of *legitimate* public interest. Second, the evaluation of newsworthiness depends on the degree of intrusion and the extent to which the plaintiff played an important role in public events, and thus on a comparison between the information revealed and the nature of the activity or event that brought the plaintiff to public attention. "Some reasonable proportion is . . . to be maintained between the events or activity that makes the individual a public figure and the private facts to which publicity is given. Revelations that may properly be made concerning a murderer or the President of the United States would not be privileged if they were to be made concerning one who is merely injured in an automobile accident." Rest.2d Torts, § 652D, com. h, p. 391.

Courts balancing these interests in cases similar to this have recognized that, when a person is involuntarily involved in a newsworthy incident, not all aspects of the person's life, and not everything the person says or does, is thereby rendered newsworthy. "Most persons are connected with some activity, vocational or avocational, as to which the public can be said as a matter of law to have a legitimate interest or curiosity. To hold as a matter of law that private facts as to such persons are also within the area of legitimate public interest could indirectly expose everyone's private life to public view." This principle is illustrated in the decisions holding that, while a particular event was newsworthy, identification of the plaintiff as the person involved, or use of the plaintiff's identifiable image, added nothing of significance to the story and was therefore an unnecessary invasion of privacy. For the same reason, a college student's candidacy for president of the student body did not render newsworthy a newspaper's revelation that the student was a transsexual, where the court could find "little if any connection between the information disclosed and [the student's] fitness for office." Similarly, a mother's private words over the body of her slain son as it lay in a hospital room were held nonnewsworthy despite undisputed legitimate public interest in the subjects of gang violence and murder.

Consistent with the above, courts have generally protected the privacy of otherwise private individual involved in events of public interest "by requiring that a logical nexus exist between the complaining individual and the matter of legitimate public interest." The contents of the publication or broadcast are protected only if they have "some substantial relevance to a matter of legitimate public interest." Thus, recent decisions have generally tested newsworthiness with regard to such individuals by assessing the logical relationship or nexus, or the lack thereof, between the events or activities that brough the person into the public eye and the particular facts disclosed. This approach accords with our own prior decisions, in that it balances the public's right to know against the plaintiff's privacy interest by drawing a protective line at the point the material revealed ceases to have any substantial connection to the subject matter of the newsworthy report. This approach also echoes the Restatement commentators' widely quoted and cited view that legitimate public interest does not include "a morbid and sensational prying into private lives *for its own sake* . . . ."

An analysis measuring newsworthiness of facts about an otherwise private person involuntarily involved in an event of public interest by their relevance to a newsworthy subject matter incorporates considerable deference to reporters and editors, avoiding the likelihood of unconstitutional interference with the freedom of the press to report truthfully on matters of legitimate public interest. In general, it is not for a court or jury to say how a particular story is best covered. The constitutional privilege to publish truthful material "ceases to operate only when an editor abuses his broad discretion to publish matters that are of legitimate public interest." By confining our interference to extreme cases, the courts "avoid[ ] unduly limiting . . . the exercise of effective editorial judgment." Nor is newsworthiness governed by the tastes or

limited interests of an individual judge or juror; a publication is newsworthy if some reasonable members of the community could entertain a legitimate interest in it. Our analysis thus does not purport to distinguish among the various legitimate purposes that may be served by truthful publications and broadcasts. As we said in *Gill v. Hearst,* "the constitutional guarantees of freedom of expression apply with equal force to the publication whether it be a news report or an entertainment feature . . . ." Thus, newsworthiness is not limited to "news" in the narrow sense of reports of current events.

On the other hand, no mode of analyzing newsworthiness can be applied mechanically or without consideration of its proper boundaries. Intensely personal or intimate revelations might not, in a given case, be considered newsworthy, especially where they bear only slight relevance to a topic of legitimate public concern.

Turning now to the case at bar, we consider whether the possibly private facts complained of here—broadly speaking, Ruth's appearance and words during the rescue and evacuation—were of legitimate public interest. We agree at the outset with defendants that the subject matter of the broadcast as a whole was of legitimate public concern. Automobile accidents are by their nature of interest to that great portion of the public that travels frequently by automobile. The rescue and medical treatment of accident victims is also of legitimate concern to much of the public, involving as it does a critical service that any member of the public may someday need. The story of Ruth's difficult extrication from the crushed car, the medical attention given her at the scene, and her evacuation by helicopter was of particular interest because it highlighted some of the challenges facing emergency workers dealing with serious accidents.

The more difficult question is whether Ruth's appearance and words as she was extricated from the overturned car, placed in the helicopter and transported to the hospital were of legitimate public concern. Pursuant to the analysis outlined earlier, we conclude the disputed material was newsworthy as a matter of law. One of the dramatic and interesting aspects of the story as a whole is its focus on flight nurse Carnahan, who appears to be in charge of communications with other emergency workers, the hospital base and Ruth, and who leads the medical assistance to Ruth at the scene. Her work is portrayed as demanding and important and as involving a measure of personal risk (e.g., in crawling under the car to aid Ruth despite warnings that gasoline may be dripping from the car). The broadcast segment makes apparent that this type of emergency care requires not only medical knowledge, concentration and courage, but an ability to talk and listen to severely traumatized patients. One of the challenges Carnahan faces in assisting Ruth is the confusion, pain and fear that Ruth understandably feels in the aftermath of the accident. For that reason the broadcast video depicting Ruth's injured physical state (which was not luridly shown) and audio showing her disorientation and despair were substantially relevant to the segment's newsworthy subject matter.

Plaintiffs argue that showing Ruth's "intimate private, medical facts and her suffering was not *necessary* to enable the public to understand the significance of the accident or the rescue as a public event." The standard, however, is not necessity. That the broadcast *could* have been edited to exclude some of Ruth's words and images and still excite a minimum degree of viewer interest is not determinative. Nor is the possibility that the members of this or another court, or a jury, might find a differently edited broadcast more to their taste or even more interesting. The courts do not, and constitutionally could not, sit as superior editors of the press.

One might argue that, while the contents of the broadcast were of legitimate interest in that they reflected on the nature and quality of emergency rescue services, the images and sounds that potentially allowed identification of Ruth as the accident victim were irrelevant and of no legitimate public interest in a broadcast that aired some months after the accident and had little or no value as "hot" news. We do not take that view. It is difficult to see how the subject broadcast could have been edited to avoid completely any possible identification without severely undercutting its legitimate descriptive and narrative impact. As broadcast, the

segment included neither Ruth's full name nor direct display of her face. She was nonetheless arguably identifiable by her first name (used in recorded dialogue), her voice, her general appearance and the recounted circumstances of the accident (which, as noted, had previously been published, with Ruth's full name and city of residence, in a newspaper). In a video documentary of this type, however, the use of that degree of truthful detail would seem not only relevant, but essential to the narrative.

II. Intrusion

[T]he action for intrusion has two elements: (1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person. We consider the elements in that order.

We ask first whether defendants "intentionally intrude[d], physically or otherwise, upon the solitude or seclusion of another," that is, into a place or conversation private to Wayne or Ruth. Cameraman Cooke's mere presence at the accident scene and filming of the events occurring there cannot be deemed either a physical or sensory intrusion on plaintiffs' seclusion. Plaintiffs had no right of ownership or possession of the property where the rescue took place, nor any actual control of the premises. Nor could they have had a reasonable expectation that members of the media would be excluded or prevented from photographing the scene; for journalists to attend and record the scenes of accidents and rescues is in no way unusual or unexpected.

Two aspects of defendants' conduct, however, raise triable issues of intrusion on seclusion. First, a triable issue exists as to whether both plaintiffs had an objectively reasonable expectation of privacy in the interior of the rescue helicopter, which served as an ambulance. Although the attendance of reporters and photographers at the scene of an accident is to be expected, we are aware of no law or custom permitting the press to ride in ambulances or enter hospital rooms during treatment without the patient's consent. (See *Noble v. Sears, Roebuck & Co.* (Cal. App. 1973), [accepting, subject to proof at trial, intrusion plaintiff's theory she had "an exclusive right of occupancy of her hospital room" as against investigator]; *Miller v. National Broadcasting Co.* (Cal. App. 1986), [Rejecting intrusion defendant's claim that plaintiff consented to media's entry into home by calling paramedics: "One seeking emergency care does not thereby 'open the door' for persons without any clearly identifiable and justifiable official reason who may wish to enter the premises where the medical aid is being administered."].) Other than the two patients and Cooke, only three people were present in the helicopter, all Mercy Air staff. As the Court of Appeal observed, "[i]t is neither the custom nor the habit of our society that any member of the public at large or its media representatives may hitch a ride in an ambulance and ogle as paramedics care for an injured stranger."

Second, Ruth was entitled to a degree of privacy in her conversations with Carnahan and other medical rescuers at the accident scene, and in Carnahan's conversations conveying medical information regarding Ruth to the hospital base. Cooke, perhaps, did not intrude into that zone of privacy merely by being present at a place where he could hear such conversations with unaided ears. But by placing a microphone on Carnahan's person, amplifying and recording what she said and heard, defendants may have listened in on conversations the parties could reasonably have expected to be private.

The Court of Appeal held plaintiffs had no reasonable expectation of privacy at the accident scene itself because the scene was within the sight and hearing of members of the public. The summary judgment record, however, does not support the Court of Appeal's conclusion; instead, it reflects, at the least, the existence of triable issues as to the privacy of certain conversations at the accident scene, as in the helicopter. The videotapes (broadcast and raw footage) show the rescue did not take place "on a heavily traveled highway," as the Court of Appeal stated, but in a ditch many yards from and below the rural superhighway, which is raised somewhat at that point to bridge a nearby crossroad. From the tapes it appears unlikely

the plaintiffs' extrication from their car and medical treatment at the scene could have been observed by any persons who, in the lower court's words, "passed by" on the roadway. Even more unlikely is that any passersby on the road could have heard Ruth's conversation with Nurse Carnahan or the other rescuers.

Whether Ruth expected her conversations with Nurse Carnahan or the other rescuers to remain private and whether any such expectation was reasonable are, on the state of the record before us, questions for the jury. We note, however, that several existing legal protections for communications could support the conclusion that Ruth possessed a reasonable expectation of privacy in her conversations with Nurse Carnahan and the other rescuers. A patient's conversation with a provider of medical care in the course of treatment including emergency treatment, carries a traditional and legally well-established expectation of privacy.

We turn to the second element of the intrusion tort, offensiveness of the intrusion. In a widely followed passage, the *Miller* court explained that determining offensiveness requires consideration of all the circumstances of the intrusion, including its degree and setting and the intruder's "motives and objectives." The *Miller* court concluded that reasonable people could regard the camera crew's conduct in filming a man's emergency medical treatment in his home, without seeking or obtaining his or his wife's consent, as showing "a cavalier disregard for ordinary citizens' rights of privacy" and, hence, as highly offensive.

We agree with the *Miller* court that all the circumstances of an intrusion, including the motives or justification of the intruder, are pertinent to the offensiveness element. Motivation or justification becomes particularly important when the intrusion is by a member of the print or broadcast press in the pursuit of news material. In deciding, therefore, whether a reporter's alleged intrusion into private matters (i.e., physical space, conversation or data) is "offensive" and hence actionable as an invasion of privacy, courts must consider the extent to which the intrusion was, under the circumstances, justified by the legitimate motive of gathering the news. Information collecting techniques that may be highly offensive when done for socially unprotected reasons—for purposes of harassment, blackmail or prurient curiosity, for example—may not be offensive to a reasonable person when employed by journalists in pursuit of a socially or politically important story. Thus, for example, "a continuous surveillance which is tortious when practiced by a creditor upon a debtor may not be tortious when practiced by media representatives in a situation where there is significant public interest [in discovery of the information sought]." Hill, *Defamation and Privacy Under the First Amendment* (1976) 76 COLUM. L. REV. 1205, 1284.

The mere fact the intruder was in pursuit of a "story" does not, however, generally justify an otherwise offensive intrusion; offensiveness depends as well on the particular method of investigation used. At one extreme, "routine . . . reporting techniques," such as asking questions of people with information ("including those with confidential or restricted information") could rarely, if ever, be deemed an actionable intrusion. At the other extreme, violation of well-established legal areas of physical or sensory privacy—trespass into a home or tapping a personal telephone line, for example—could rarely, if ever, be justified by a reporter's need to get the story. Such acts would be deemed highly offensive even if the information sought was of weighty public concern; they would also be outside any protection the Constitution provides to newsgathering.

On this summary judgment record, we believe a jury could find defendants' recording of Ruth's communications to Carnahan and other rescuers, and filming in the air ambulance, to be "highly offensive to a reasonable person." With regard to the depth of the intrusion, a reasonable jury could find highly offensive the placement of a microphone on a medical rescuer in order to intercept what would otherwise be private conversations with an injured patient. In that setting, as defendants could and should have foreseen, the patient would not know her words were being recorded and would not have occasion to ask about, and object or consent to,

recording. Defendants, it could reasonably be said, took calculated advantage of the patient's "vulnerability and confusion."

For much the same reason, a jury could reasonably regard entering and riding in an ambulance—whether on the ground or in the air—with two seriously injured patients to be an egregious intrusion on a place of expected seclusion. Again, the patients, at least in this case, were hardly in a position to keep careful watch on who was riding with them, or to inquire as to everyone's business and consent or object to their presence. A jury could reasonably believe that fundamental respect for human dignity requires the patients' anxious journey be taken only with those whose care is solely for them and out of sight of the prying eyes (or cameras) of others.

CHIN, Justice, concurring and dissenting.

I dissent, however, from the plurality's holding that plaintiffs' " intrusion" cause of action should be remanded for trial. The critical question is whether defendants' privacy intrusion was "*highly* offensive to a reasonable person." Ruth's expectations notwithstanding, I do not believe that a reasonable trier of fact could find that defendants' conduct in this case was "highly offensive to a reasonable person," the test adopted by the plurality. Plaintiffs do not allege that defendants, though present at the accident rescue scene and in the helicopter, interfered with either the rescue or medical efforts, elicited embarrassing or offensive information from plaintiffs, or even tried to interrogate or interview them. Defendants' news team evidently merely recorded newsworthy events "of legitimate public concern" as they transpired. Defendants' apparent motive in undertaking the supposed privacy invasion was a reasonable and nonmalicious one: to obtain an accurate depiction of the rescue efforts from start to finish. The event was newsworthy, and the ultimate broadcast was both dramatic and educational, rather than tawdry or embarrassing.

No illegal trespass on private property occurred, and any technical illegality arising from defendants' recording Ruth's conversations with medical personnel was not so "highly offensive" as to justify liability. Recording the innocuous, inoffensive conversations that occurred between Ruth and the nurse assisting her and filming the seemingly routine, though certainly newsworthy, helicopter ride may have technically invaded plaintiffs' private "space," but in my view no "highly offensive" invasion of their privacy occurred.

[H]ere the broadcast showed Ruth speaking in settings where others could hear her, and the fact that she did not realize she was being recorded does not ipso facto transform defendants' newsgathering procedures into *highly* offensive conduct within the meaning of the law of intrusion.

BROWN, Justice, concurring and dissenting.

In this case, a straightforward application of the *Kapellas v. Kofman* (Cal. 1969) newsworthiness test leads to one inescapable conclusion—that, at the very least, there are triable issues of material fact on the question of newsworthiness. The private facts broadcast had little, if any, social value. The public has no legitimate interest in witnessing Ruth's disorientation and despair. Nor does it have any legitimate interest in knowing Ruth's personal and innermost thoughts immediately after sustaining injuries that rendered her a paraplegic and left her hospitalized for months—"I just want to die. I don't want to go through this." The depth of the broadcast's intrusion into ostensibly private affairs was substantial. As the plurality later acknowledges in analyzing "the depth of the intrusion" for purposes of Ruth's intrusion cause of action, "[a]rguably, the last thing an injured accident victim should have to worry about while being pried from her wrecked car is that a television producer may be recording everything she says to medical personnel for the possible edification and entertainment of casual television viewers."

Inexplicably, the plurality jettisons the *Kapellas* newsworthiness test [which considers proportionality] in favor of its own "logical relationship" test. Under this new test, "where the facts disclosed about a private person involuntarily caught up in events of public interest bear a logical relationship to the newsworthy subject of the broadcast and are not intrusive in great disproportion to their relevance—the broadcast was of legitimate public concern, barring liability under the private facts tort." Here, the plurality misapplies its own new test, wrongly concluding there are no triable issues of material fact.

Under the plurality's new test, personal privacy must yield whenever the overall subject matter of a broadcast is newsworthy and the private facts disclosed bear a "logical relationship" to that subject matter. Thus, to "[t]he more difficult question [of] whether Ruth's appearance and words as she was extricated from the overturned car, placed in the helicopter and transported to the hospital were of legitimate public concern," the plurality offers the facile answer that they were because "her disorientation and despair were substantially relevant to the segment's newsworthy subject matter."

Contrary to the plurality's claim that it is "*accommodating* conflicting interests in personal privacy and in press freedom as guaranteed by the First Amendment to the United States' Constitution," in reality, it sacrifices the constitutional right to privacy on the altar of the First Amendment.

Notes

1. Readers might be wondering if this conduct violates HIPAA. It does. However, this case predates HIPAA, so that legal regime is not available.
2. Most commonly, courts assessing newsworthiness use a variant of a logical and proportional nexus test. The private fact being disclosed must be relevant to the newsworthiness of the story, and there must not be a gross disproportionality between that relevance and the magnitude of the privacy invasion. In the words of the Shulman majority: "The standard, however, is not necessity." And, as Brown's dissent highlights, gross disproportionality can be quite difficult to prove.

Y.G. v. Jewish Hospital of St. Louis, 795 S.W.2d 488 (Mo. App. 1990)

JOSEPH J. SIMEONE, Senior Judge.

These proceedings involve the common law tort of an alleged invasion of the privacy of the plaintiffs-appellants, Y.G. and L.G., husband and wife. This complex, important case of first impression requires us to decide the precise issue of resolving the delicate balance between a married couple's right to their privacy in procreating children by the process of *in vitro* fertilization and the privilege or freedom of a hospital where such procedures are done, and the freedom of the electronic news media to report and make public the events surrounding the modern medical "miracle" of the extraordinary process *in vitro* fertilization.

The issue is certainly not easily resolved for the cherished freedoms embodied in the American ideal of privacy of the individual and the freedom of the news media necessarily conflict. On the one hand, private individuals in the plight of these unnamed plaintiffs to keep their bodily procreative secrets known only to their parents or certain close friends is of the highest importance to them, and on the other hand, the news media has a privilege and often a duty to report to the public certain "newsworthy" events which are of great interest to the general public.

The first amended petition filed on June 20, 1989, stated that Y.G. and L.G. are husband and wife and residents of St. Louis County. The petition alleged that the wife, L.G., was five months pregnant, bearing triplets "conceived through a medical process known as *in vitro* fertilization at and under the auspices of [Jewish Hospital]." The hospital had planned to have a "social function" and a "meeting of [the] couples" presently and previously involved in its *in*

vitro program which would be held on September 11, 1988, to commemorate the fifth anniversary of the *in vitro* fertilization program at the hospital. Plaintiffs were invited to this "social gathering" and "meeting." The petition specifically alleged that the hospital "assured" them that no "publicity nor public exposure of persons attending" the function would occur. At the invitation of the Hospital, plaintiffs attended the "function." The plaintiffs alleged that at that "function" a "film and reporting news team of KSDK was present." Plaintiffs were twice requested to give an interview on television film but each time they refused, and made every "reasonable effort" to avoid being filmed or interviewed by the representatives of the electronic media.

Before the social function of *in vitro* procedure, plaintiffs had “told no one” about their attempt to procreate, other than Y.G.'s mother. The petition then alleged that “without permission,” and after having been denied “express permission, waiver or privilege, KSDK filmed the function and showed it on their television program that evening . . . [that] L.G. [and Y.G.] were present at [the] Hospital's function, . . . and the newscast [although not mentioning their names] told [that they were] expecting triplets by reason of their participation in [the] Hospital's *in vitro* program.”

The petition concluded that the "acts" of defendants constituted an invasion of plaintiffs' privacy. Plaintiffs' identification as parents of triplets conceived through the *in vitro* program was a private matter in which the public had no legitimate concern. The “acts of defendants damaged Plaintiffs by loss of their privacy, by embarrassment and by ridicule . . . by those who viewed” the news program of KSDK, and that the “acts of defendants were such to bring humiliation or shame to a person of ordinarily sensibilities.” Plaintiffs prayed for actual and punitive damages. An affidavit by Y.G. was filed with the petition. The affidavit stated that after the televised broadcast, she received numerous calls, and embarrassing questions and in addition was chastised by her church. The husband's affidavit stated he was ridiculed at work. Implicit in the petition is the fact that KSDK was informed of the September 1988 function and was invited to attend the function.

On August 25, 1989, Jewish Hospital filed its motion to dismiss for failure to state a claim upon which relief could be granted because (a) it "did not publicize the events" mentioned in the petition, (b) the televised report was of legitimate concern to the public, (c) it "had no reason to expect that the report prepared by KSDK would be highly offensive to a reasonable person," and (d) plaintiffs waived "whatever right of privacy they had by attending the function in the company of third party non-medical personnel." KSDK also filed a motion to dismiss for failure to state a claim contending that its "report was of legitimate concern to the public," "that it had no reason to believe that the report would be highly offensive to a reasonable person," and plaintiffs waived "whatever right of privacy they had by attending the September 11, 1988 party."

Attached to the motion filed by KSDK were certain affidavits stating that the topics of infertility, and procreative technology, including *in vitro* fertilization have been regularly featured in news reports by both print and electronic media. Various news reports were attached. The executive secretary for KSDK attached a videotape copy of the video broadcast taken at the hospital on September 12, 1990. The reporter for KSDK also made an affidavit. In the affidavit she stated that Jewish Hospital invited KSDK to attend and report on the "party" the hospital was holding. She attended the "party" and prepared the TV report which was broadcast on the 10:00 p.m. news. The plaintiffs appeared on camera for approximately three seconds.

KSDK's brief contends that their report was a matter of legitimate concern to the public, that plaintiffs' "fleeting appearance" was not a private matter and was not a "public disclosure of private facts;" it was not highly offensive and that the plaintiffs waived whatever right of privacy they had by attending the "party."

After the motions were argued, the trial court, on October 31, 1989 sustained the "motions to dismiss" filed by both Jewish Hospital and KSDK.

Although there were earlier English and American decisions obliquely construing the right of privacy by way of equitable relief, it was not until the seminal, classic article of Samuel D. Warren and Louis D. Brandeis, *The Right of Privacy,* 4 HARV. L. REV. 193 (1890), that first argued for, recognized and gave impetus to the modern tort of invasion of privacy. The constitutional doctrines of "right of privacy" involving abortion, use of contraceptives or sexual orientation are not to be equated with the common law tort for the invasion of privacy alleged here.

Missouri was one of the first states to give legal recognition to the "new" tort of the right of privacy. *Munden v. Harris* (Mo. App. 1911). In *Munden,* defendants published a photograph of a five-year-old boy to advertise their merchandise. The defendants demurred, and the demurrer was sustained. However, the "Kansas City Court of Appeals" refusing to follow earlier cases, in other jurisdictions, stated:

> The right of privacy is spoken of as a new right, when in fact it is an old right with a new name. Life, liberty and the pursuit of happiness are rights of all [persons] . . . The right to life includes the right to enjoy life. Everyone has the privilege of following that mode of life, if it will not interfere with others, which will bring to him the most contentment and happiness. He may adopt that of privacy, or if he likes, of entire seclusion . . . . If this right is invaded, he may have his remedy, either by restraint in equity or damages in an action at law.

The elements of an action for publication of a private matter are (1) publication or "publicity," (2) absent any waiver or privilege, (3) of private matters in which the public has no legitimate concern, (4) so as to bring shame or humiliation to a person of ordinary sensibilities.

In *Buller v. Pulitzer Pub. Co* (Mo. App. 1984), this court per Judge Kelly discussed the elements of the tort and recognized that the Restatement distinctions have been adopted in Missouri, by use, if not by express language.

In *Williams v. KCMO Broadcasting Division-Meredith Corporation* (Mo. App. 1971), the court held that where the plaintiff was arrested by mistake and the arrest was televised, the plaintiff was involved in a noteworthy event about which the public had a right to be informed. The *Williams* court distinguished this type of situation from one in which a woman's dress was blown up over her waist in public and she had been photographed, and another in which a man's injuries sustained on the job had been photographed by his employer and shown at safety meetings. Neither of these were held to be items of legitimate public interest and therefore created a cause of action for the invasion of right of privacy. In *Barber v. Time* (Mo. 1942), the fact that plaintiff had entered a hospital for treatment of an eating disorder was held to be a private interest.

From these and other decisions, we believe it is clear that where the operation of laws and the activities of the police or other public bodies are involved, the matter is within the public interest. Where, however, events occur which affect the individual alone, and do not touch the sphere of public concern, they are not within the public interest.

The tort of invasion of privacy by public disclosure of a private matter requires that the fact disclosed must be a "private matter" in which the public has no legitimate concern. The determination of this fact is a matter for the court to decide and once the court has determined the matter is private, and there is substantial evidence of unreasonable interference with the private matter, the case is for the jury.

This element is often described as "newsworthiness," although it encompasses more than that. Judicial decisions have held that certain details of a person's life may fall into the public interest through legal action, police activity or the action of other public bodies. For example,

matters become the subject of legitimate public concern when they are included in open court records, or are the focus of police arrest, even if no charges follow, or when they involve criminal action of which the police should be informed, Similarly, dissemination of an event that occurred in public view is not a private matter. Generally stated, there can be no invasion of privacy in giving further publicity to a matter which is already public.

But where a peculiarly private matter is concerned, the situation is entirely different. In analogous decisions, the right of privacy has been held to apply particularly to sexual matters or matters of procreation. Publication of sexual matters have been held actionable under the invasion of privacy tort.

The Missouri Supreme Court held that a person's medical treatment is a private matter in *Barber*. In *Barber,* the court said in determining whether the case presented a jury issue, the court stated "certainly if there is any right of privacy at all, it should include the right to obtain medical treatment at home or in a hospital for an individual personal condition (at least if it is not contagious or dangerous to others) without personal publicity." The court held that although plaintiff's medical condition may have been a matter of public interest because it was unusual, her identity was a private matter protected by the right of privacy.

This distinction between a "newsworthy event" and publication of a purely private matter is applicable to the case at bar. The *in vitro* program and its success may well have been matters of public interest, but the identity of the plaintiffs participating in the program was, we conclude, a private matter. It did concern matters of procreation and sexual relations as well as medical treatment—all private matters. The *in vitro* fertilization program participation was certainly not a matter of public record nor did it become of public concern due to any of the ordinary incidents of public concern. Consequently, we hold that plaintiffs' identity was a private matter which was not newsworthy nor a matter of public record.

Tested within all these principles, authorities, decisions and the policies of the right of privacy and balancing the interests of the media to publish "newsworthy" events, and after the most careful consideration of the facts of this case, we conclude that plaintiffs' interests outweigh the interests of the defendants and plaintiffs should be given an opportunity to prove their case in a trial, and that all the elements necessary to maintain an action for invasion of privacy listed in the Restatement and the Missouri cases are satisfied, at least at this stage of the proceedings. Plaintiffs' participation in the program was a private matter. There was a "publication" or "publicity" of private facts; there was no waiver as a matter of law on the part of the plaintiffs; the petition alleges that the plaintiffs suffered humiliation and embarrassment and the issue of whether the matter was one in which the public has no legitimate concern as to these particular plaintiffs should be determined under a procedure other than a motion to dismiss or summary judgment.

The plaintiffs alleged in their petition that they were "assured" that "no publicity nor public exposure" would occur, that they twice refused interviews or to be filmed, and made every reasonable effort to avoid being filmed, and that no one knew of their reproductive process other than Y.G.'s mother. They stated that the function dealing with the *in vitro* function was a "private" affair in which the public had no legitimate interest. Viewing the petition in the most favorable light, we hold that it states a claim upon which relief may be granted. Implicit in the petition is an allegation that Jewish Hospital either invited KSDK to be present or informed the media that the event was to take place in September 1988. Moreover, the KSDK reporter's affidavit explicitly stated that KSDK was "invited" by Jewish Hospital to attend and report on a party the hospital was holding on September 11, 1988.

While the modern medical, technical process of *in vitro* fertilization may be of great interest to the public generally, publicizing the individual persons who undergo such medical "miracle," without their consent and without waiver states a claim upon which relief may be granted.

The defendants contend that the plaintiffs waived any right to privacy they had by attending the function. As to waiver by attending the function, we hold that there was no waiver. Plaintiffs were assured that the function would be private, they twice refused an interview, and by merely attending the function there was no express voluntary waiver of a known right.

KSDK's motion alleged that appellants waived their right to privacy by attending the party because they disclosed their *in vitro* program participation to the other attendees. Respondent cites *Gill v. Hearst Publishing Co.* (Cal. 1953), for the proposition that a person photographed while open to public view has no privacy cause of action upon publication of that photograph. The *Gill* court stated that the photograph of an amorous couple in a public park did not disclose anything which until then had been private but rather only extended knowledge of the particular incident to a somewhat larger public than had actually witnessed it at the time of occurrence. There are numerous cases holding that matters of public record or events taking place in a public location may be publicized without invasion of privacy.

The mere fact that an event takes place where others are present does not waive the right to privacy. *Stessman v. A.M. Black Hawk Broadcasting* (Iowa 1987) (dismissal of privacy action improper where plaintiff filmed in public restaurant may have been in private dining area). Similarly, disclosing private facts to an individual, even a member of the press, is not "consent" to publication since a "selective disclosure" is "based on a judgment as to whether knowledge by that person would be felt to be objectionable." *See Hawkins by Hawkins v. Multimedia, Inc.* (S.C. 1986) (no consent to publication where plaintiff did not terminate conversation with reporter immediately, but talked for only a few minutes and was never told he would be identified in an article).

The difference between those situations where privacy is waived and those where it is preserved, at least in the news media context, may best be summed by Judge O'Neill's comment in *Rafferty v. Hartford Courant Co.* (Conn. 1980):

> A newspaper can, at best, claim only to be one of the public. It has the same 'right to find out' as the rest of the public. It has the same right to publish as the rest of the public. It has no greater right to intrude to obtain information than each citizen has because each citizen has the same right to publish.

In the case at bar, the allegations of the petition show that appellants were assured that the persons invited would include only other persons involved in the IVF program, and would not be open to the public or the media. By attending such a function, appellants clearly chose to disclose their participation to only the other *in vitro* couples. By so attending this limited gathering, they did not waive their right to keep their condition and the process of *in vitro* private, in respect to the general public.

Respondents contend that the appellants appeared in the news report only for a few fleeting seconds. But it is not the time that is relevant, but the fact that they did appear on the news report and were recognized by friends and acquaintances.

In addition, we cannot hold that attendance at the gathering constituted an appearance in a public place so as to subject appellants to publicity.

Defendants contend that the television report would not and did not bring shame or humiliation to an ordinary person. We believe this to be a factual question which the jury should resolve, and which is not appropriate to determine upon a motion to dismiss or upon summary judgment.

Respondents, citing *Benally v. Hundred Arrows Press, Inc.* (D.N.M. 1985), place great emphasis on the fact that a large part of appellants' distress stemmed from their religious affiliations and argue that appellants are extra-sensitive. It is not clear whether a reasonable person would be insensitive by disclosure of his participation in the program. The implications

of this participation, and the physical problems which exist with the couple's reproductive systems or that they are incapable of performing sexually, are matters that could embarrass a reasonable person, and such matters should be left for a factual determination.

CARL R. GAERTNER, Presiding Judge, dissenting.

I respectfully dissent. At the outset I believe it is important to recognize we are concerned with publication of a newsworthy event, a gathering to celebrate five years of successful participation in a "miracle" of modern medical science. There is no contention the publication was inaccurate, defamatory, sensational or lacking in good taste. Plaintiffs were not identified by name nor singled out for special treatment such as a lingering close-up or an isolated picture of them apart from the large group of attendees. Their complaint is predicated solely upon their subjective desire to conceal their participation in an undeniably newsworthy program.

The exhaustive discussion in the majority opinion of the history and development of the tort of invasion of privacy demonstrates that liability for publication of private matters is dependent not upon the subjective view of the individual, but rather upon the more objective standard of reasonableness. This objective standard, in my opinion, encompasses each of the elements under consideration: the reasonableness of plaintiffs' expectation of privacy, the reasonableness of defendants' awareness that publication would be highly offensive, the reasonableness of defendants' belief the matter is of legitimate concern to the public. Is it reasonable for plaintiffs to volunteer for participation in the *in vitro* Fertilization Project, a matter of widespread, international publicity, without recognition of the likelihood of disclosure? Is it reasonable for plaintiffs to accept the invitation to attend the five-year celebration of the program without awareness that their participation would be made known to all those in attendance as well as all who observe them entering and leaving the gathering? Is it reasonable for plaintiffs to maintain an expectation of privacy when, after seeing the cameras and refusing to be interviewed, they remain in the midst of the group of approximately forty people who were all being filmed without objection rather than stepping to the side of the room until the camera was lowered? In my opinion, each question, viewed individually and certainly when considered collectively, requires a negative answer. I do not believe reasonable minds could avoid concluding that by their conduct plaintiffs waived any right of privacy they may have subjectively desired.

Reasonableness is also the hallmark by which the conduct of defendants must be tested. Plaintiffs do not suggest any impropriety in the publicity given to the celebration of the achievements of five years of successful *in vitro* Fertilization. Assuming the truth of plaintiffs' allegations regarding their refusal to be interviewed, can defendants be charged with the realization that filming plaintiffs in the midst of the entire group of celebrants would constitute a publication causing humiliation to a person of reasonable sensibilities. Having scrupulously observed plaintiffs' request not to be interviewed, does the showing of plaintiffs' faces for three seconds in the midst of a group at a newsworthy affair without identification, close-up or other singling out "show a serious, unreasonable, unwarranted and offensive interference with the individual's private affairs?" I think not. "The law does not protect the overly sensitive, and if a reasonable person would not be humiliated by the publicity, no recovery can be had."

Finally, the question of legitimate public interest must be viewed through the eyes of a reasonable person. The multitude of cases cited in the majority opinion clearly demonstrates that an individual's desire of privacy may be frustrated merely because of his innocent, unintentional involvement in a newsworthy event of legitimate public interest. It seems to me the attempt by the majority to distinguish between the appropriate public interest in the subject of *in vitro* Fertilization and the illegitimate public interest in plaintiffs' participation therein is vitiated by these authorities. This is particularly true in light of the truly remarkable fact that not one but three fertilized ova were implanted. I do not believe reasonable minds could differ

upon the newsworthiness or legitimate public interest in plaintiffs' involvement in such a scientific accomplishment.

Notes

1. This case turns upon consent, reasonable expectations, and newsworthiness. How private did the couple have to be to maintain their privacy rights? Merely getting medical treatment does not relinquish the couple's privacy rights, yet the court was divided about whether attending this optional social event related to their medical treatment does. The dissent thinks it is reasonable to ask a privacy-concerned individual to leave an event that contains reporters and news cameras. The majority thinks the connection to the hospital, the private nature of the medical facts, and the previous privacy promises are enough to counteract that.
2. Another issue raised here is that of small group privacy. Consider support groups like Alcoholics Anonymous, Narcotics Anonymous, and bereavement groups. People come together with near strangers and disclose highly personal information. Is this information still private? The most likely answer is "yes," but courts struggle to agree on a coherent rationale. In general, however, they will consider the strength and content of the confidentiality norms of the group.
3. Certainly it would have been better had the reporters either omitted or blurred the faces of the couple in their ultimate broadcast; neither the hospital nor the news organization make the argument that the Gees themselves were newsworthy. But, as with *Shulman*, here we have an issue of care. Was it the news organization's responsibility to protect the privacy of the Gees? If news organization need to take an extra level of care, fewer stories will get written – think of the extra legal and video editing hours that would be required. If the responsibility of care is instead placed on the Gees, then news organizations need devote fewer resources to protecting privacy but everyday people need to be more cautious in their daily lives.
4. Is this couple committing social fraud? They were part of a religion that disapproved of IVF. By getting IVF and keeping it secret, the couple got to pretend to be rule-abiding members of their religion while still getting the benefits of the forbidden procedure. This raises a host of hard moral questions from both the pro-IVF and anti-IVF sides.
   This type of issue has arisen repeatedly over the years. In the 1990s and early 2000s, there was considerable debate over whether it was good to expose that conservative and sometimes anti-gay political figures were themselves gay. There has also been discussion of outing people who have had (or asked their partners or family members to have) abortions while being opposed to abortion rights.

3) Republisher Immunity

Sipple v. Chronicle Publishing Co., 154 Cal.App.3d 1040 (1984)

CALDECOTT, Presiding Justice.

On September 22, 1975, Sara Jane Moore attempted to assassinate President Gerald R. Ford while the latter was visiting San Francisco, California. Plaintiff Oliver W. Sipple . . . who was in the crowd at Union Square, San Francisco, grabbed or struck Moore's arm as the latter was about to fire the gun and shoot at the President. Although no one can be certain whether or not Sipple actually saved the President's life, the assassination attempt did not succeed and Sipple was considered a hero for his selfless action and was subject to significant publicity throughout the nation following the assassination attempt.

Among the many articles concerning the event was a column, written by Herb Caen and published by the San Francisco Chronicle on September 24, 1975. The article read in part as follows: "One of the heroes of the day, Oliver 'Bill' Sipple, the ex-Marine who grabbed Sara Jane

Moore's arm just as her gun was fired and thereby may have saved the President's life, was the center of midnight attention at the Red Lantern, a Golden Gate Ave. bar he favors. The Rev. Ray Broshears, head of Helping Hands, and Gay Politico, Harvey Milk, who claim to be among Sipple's close friends, describe themselves as 'proud—maybe this will help break the stereotype.' Sipple is among the workers in Milk's campaign for Supervisor."

Thereafter, the Los Angeles Times and numerous out-of-state newspapers published articles which referring to the primary source, (i.e., the story published in the San Francisco Chronicle) mentioned both the heroic act shown by Sipple and the fact that he was a prominent member of the San Francisco gay community. Some of those articles speculated that President Ford's failure to promptly thank Sipple for his heroic act was a result of Sipple's sexual orientation.[1]

Finding the articles offensive to his private life, on September 30, 1975, Sipple filed an action against the California defendants, the Chronicle Publishing Company, Charles de Young Thieriot, the publisher of the Chronicle, Herb Caen, a columnist for the Chronicle, The Times Mirror Company, the owner and publisher of the Los Angeles Times, and Otis Chandler (hereafter together respondents) and numerous out-of-state newspapers. The complaint was predicated upon the theory of invasion of privacy and alleged in essence that defendants without authorization and consent published private facts about plaintiff's life by disclosing that plaintiff was homosexual in his personal and private sexual orientation; that said publications were highly offensive to plaintiff inasmuch as his parents, brothers and sisters learned for the first time of his homosexual orientation; and that as a consequence of disclosure of private facts about his life plaintiff was abandoned by his family, exposed to contempt and ridicule causing him great mental anguish, embarrassment and humiliation. Plaintiff finally alleged that defendants' conduct amounted to malice and oppression calling for both compensatory and punitive damages.

[R]espondents renewed their motion for summary judgment claiming in essence that the information disclosed in the articles was already public; that the publication was newsworthy which provided immunity for invasion of privacy; and that the element of malice was likewise absent.

[T]he summary judgment in this case must be upheld on two grounds. First, as appears from the record properly considered for the purposes of summary judgment, the facts disclosed by the articles were not private facts within the meaning of the law. Second, the record likewise reveals on its face that the publications in dispute were newsworthy and thus constituted a protective shield from liability based upon invasion of privacy.

(A) *The facts published were not private.*

[A] crucial ingredient of the tort premised upon invasion of one's privacy is a public disclosure of *private facts,* that is the unwarranted publication of intimate details of one's private life which are outside the realm of legitimate public interest. In elaborating on the

---

[1] For example, the September 25, 1975, issue of the Los Angeles Times wrote inter alia as follows: "A husky ex-marine who was a hero in the attempted assassination of President Ford emerged Wednesday as a prominent figure in the gay community."

"And questions were raised in the gay community if Oliver (Bill) Sipple, 32, was being shunned by the White House because of his associations."

"Sipple, who lunged at Sara Jane Moore and deflected her revolver as she fired at the President, conceded that he is a member of the 'court' of Mike Caringi, who was elected 'emperor of San Francisco' by the gay community."

"A column item in a morning newspaper here strongly implied Wednesday that Sipple is gay."

"Harvey Milk, a prominent member of this city's large homosexual community and a longtime friend of Sipple, speculated Wednesday that the absence of a phone call or telegram of gratitude from the White House might not be just an oversight."

notion, the cases explain that there can be no privacy with respect to a matter which is already public or which has previously become part of the "public domain." Moreover, it is equally underlined that there is no liability when the defendant merely gives further publicity to information about the plaintiff which is already public or when the further publicity relates to matters which the plaintiff leaves open to the public eye.

The undisputed facts reveal that prior to the publication of the newspaper articles in question appellant's homosexual orientation and participation in gay community activities had been known by hundreds of people in a variety of cities, including New York, Dallas, Houston, San Diego, Los Angeles and San Francisco. Thus, appellant's deposition shows that prior to the assassination attempt appellant spent a lot of time in "Tenderloin" and "Castro," the well-known gay sections of San Francisco; that he frequented gay bars and other homosexual gatherings in both San Francisco and other cities; that he marched in gay parades on several occasions; that he supported the campaign of Mike Caringi for the election of "Emperor"; that he participated in the coronation of the "Emperor" and sat at Caringi's table on that occasion; that his friendship with Harvey Milk, another prominent gay, was well-known and publicized in gay newspapers; and that his homosexual association and name had been reported in gay magazines (such as Data Boy, Pacific Coast Times, Male Express, etc.) several times before the publications in question. In fact, appellant quite candidly conceded that he did not make a secret of his being a homosexual and that if anyone would ask, he would frankly admit that he was gay. In short, since appellant's sexual orientation was already in public domain and since the articles in question did no more than to give further publicity to matters which appellant left open to the eye of the public, a vital element of the tort was missing rendering it vulnerable to summary disposal.

Although the conclusion reached above applies with equal force to all respondents, we cannot help observing that respondents Times Mirror and its editor are exempt from liability on the additional ground that the Los Angeles Times only republished the Chronicle article which implied that appellant was gay. It is, of course, axiomatic that no right of privacy attaches to a matter of general interest that has already been publicly released in a periodical or in a newspaper of local or regional circulation.

(B) *The publication was newsworthy.*

But even aside from the aforegoing considerations, the summary judgment dismissing the action against respondents was justified on the additional, independent basis that the publication contained in the articles in dispute was newsworthy.

As referred to above, our courts have recognized a broad privilege cloaking the truthful publication of all newsworthy matters. Thus, our Supreme Court stated that a truthful publication is protected if (1) it is newsworthy and (2) it does not reveal facts so offensive as to shock the community notions of decency. While it has been said that the general criteria for determining newsworthiness are (a) the social value of the facts published; (b) the depth of the article's intrusion into ostensibly private affairs; and (c) the extent to which the individual voluntarily acceded to a position of public notoriety, the cases and authorities further explain that the paramount test of newsworthiness is whether the matter is of legitimate public interest which in turn must be determined according to the community mores. "In determining what is a matter of legitimate public interest, account must be taken of the customs and conventions of the community; and in the last analysis what is proper becomes a matter of the community mores. *The line is to be drawn when the publicity ceases to be the giving of information to which the public is entitled, and becomes a morbid and sensational prying into private lives for its own sake,* with which a reasonable member of the public, with decent standards, would say that he had no concern." Accord, Rest., 2d Torts, § 652D, com. h.

In the case at bench the publication of appellant's homosexual orientation which had already been widely known by many people in a number of communities was not so offensive

even at the time of the publication as to shock the community notions of decency. Moreover, and perhaps even more to the point, the record shows that the publications were not motivated by a morbid and sensational prying into appellant's private life but rather were prompted by legitimate political considerations, i.e., to dispel the false public opinion that gays were timid, weak and unheroic figures and to raise the equally important political question whether the President of the United States entertained a discriminatory attitude or bias against a minority group such as homosexuals. Thus appellant's case squarely falls within the language of *Kapellas* in which the California Supreme Court emphasized that "when, [as here] the legitimate public interest in the published information is substantial, a much greater intrusion into an individual's private life will be sanctioned, especially if the individual willingly entered into the public sphere."

Appellant's contention that by saving the President's life he did not intend to enter into the limelight and become a public figure, can be easily answered. In elaborating on involuntary public figures, Restatement Second of Torts section 625D, comment f, sets out in part as follows: "There are other individuals who have not sought publicity or consented to it, but through their own conduct or otherwise have become a legitimate subject of public interest. They have, in other words, become 'news.' . . . These persons are regarded as properly subject to the public interest, and publishers are permitted to satisfy the curiosity of the public as to its heroes, leaders, villains and victims, and those who are closely associated with them. As in the case of the voluntary public figure, the authorized publicity is not limited to the event that itself arouses the public interest, and to some reasonable extent includes publicity given to facts about the individual that would otherwise be purely private."

In summary, appellant's assertion notwithstanding, the trial court could determine as a matter of law that the facts contained in the articles were not private facts within the purview of the law and also that the publications relative to the appellant were newsworthy.

Notes

1. Some reports state that Sipple never fully reconciled with his parents after his sexual orientation was revealed to them, and that his father did not allow him to attend his mother's funeral. As for the president, Ford wrote him a letter praising Sipple for his heroic deed. Sipple replied to that letter, thanking the president and asking if the president could call Sipple's parents. There is no record of Ford making that call.[22] Sipple did, however, keep Ford's letter framed in his apartment.[23]
2. In a world where much is published in obscure corners of the internet, the doctrine of republisher immunity can easily stand as a bar to recovery when a major publication takes what was previously hidden and makes it widely known. Imagine your ex-lover wrote a blog post about you or has an old Instagram or TikTok post describing the details of your breakup. If they have few followers then the post could remain unknown even to your close associates. Yet it is still available to the public and could block a lawsuit were CNN to find and republish it in time for your Senate confirmation hearing.
3. Consider the implications of the separate newsworthiness analysis here. Sipple's sexual orientation was newsworthy because of the combination of his actions and his identity. One could similarly point to a 1990 *New York Times* article entitled "First Black Elected to Head Harvard's Law Review." President (of *Harvard Law Review*) Barack Obama's identity was

[22] *Transcript: Oliver Sipple*, RADIOLAB, Sept. 22, 2017, https://www.radiolab.org/podcast/oliver-sipple/transcript.

[23] Lynne Duke, *Caught in Fate's Trajectory, Along with Gerald Ford*, WASH. POST, Dec. 31, 2006, https://www.washingtonpost.com/wp-dyn/content/article/2006/12/30/AR2006123000160.html. The article also includes claims from Sipple's brother that Sipple's parents came to accept him again, which is inconsistent with Sipple not being allowed to attend his mother's funeral. Since Sipple died in 1989, there does not appear to be a way to reconcile these conflicting accounts.

notable because it challenged a prevailing stereotype. Similarly and more recently, *The Michigan Daily* published a 2018 article entitled "Michigan Law student becomes first Black Editor-in-Chief."[24]

Some people enjoy public attention and likely are happy to serve as standard bearers for their identity groups. Others, such as Sipple, would prefer to not. The newsworthiness analysis of the *Sipple* case suggests that people do not have much of a choice, however.

4. If it is newsworthy to challenge a stereotype, is it also newsworthy to confirm it? Would that not also inform the public debate? If we are comfortable with saying that a man's heroism makes his sexual orientation newsworthy, would that also mean we should be comfortable with his cowardice making it newsworthy?

   This feeds into a broader question about distributive privacy costs. If a person from a stigmatized or small group does newsworthy things, it will be easy to argue that their stigmatized or rare identity is a newsworthy part of that. The same people will then regularly find their privacy rights limited by the inherent newsworthiness of their existence.

4) First Amendment Limitations on Public Disclosure Liability

Privacy enjoys a complicated relationship with freedom of speech. The law is restricting one person's freedom of speech whenever it requires them to keep another person's secrets. Yet privacy also permits speech, allowing for people to share unfiltered opinions with their friends, their doctors, and people bound by non-disclosure agreements. It can allow people to seek out information secretly and to share it anonymously. This promotes speech and freethinking.

The complex relationship between privacy and freedom of speech is illuminated not at all by the text of the First Amendment:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Congress (and the states) regularly make laws that abridge the freedom of speech and courts regularly uphold these laws. Freedom of speech will not allow you to distribute child pornography, military officials to leak classified documents, or Alex Jones to defame the families of Sandy Hook. To allow for these results, the Supreme Court has created a complicated jurisprudence built around the idea that the First Amendment does not mean what it says. To oversimplify current doctrine:

- Certain forms of expression (child pornography, obscenity, fighting words) receive no protection under the First Amendment.
- Content-neutral regulations are generally reviewed under intermediate scrutiny. To pass intermediate scrutiny, a law must be "narrowly tailored" to promote a "substantial" government interest.
- Content-based restrictions are generally subjected to strict scrutiny, meaning that the law must be the "least restrictive means" to achieve a "compelling" state interest.

The most challenging Supreme Court cases push at the boundaries of these categories. Is this child pornography, and thus unprotected? Is that regulation content-based, and therefore must satisfy the notoriously difficult test of strict scrutiny, or is it content-neutral, requiring only intermediate scrutiny?

[24] Regarding Megan Brown, who has not yet been elected president but still has several decades.

In addition to being directly relevant to the tort of public disclosure of public facts, the following cases also inform our understandings of laws regulating image-based sexual abuse (also known as nonconsensual pornography), harassment, and doxing.

The first two cases below predate the formalization of the current doctrinal categories, so do not expect to see the above terminology. One you reach *Bartnicki*, however, it will be present.

Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975)

Mr. Justice WHITE delivered the opinion of the Court.

The issue before us in this case is whether, consistently with the First and Fourteenth Amendments, a State may extend a cause of action for damages for invasion of privacy caused by the publication of the name of a deceased rape victim which was publicly revealed in connection with the prosecution of the crime.

In August 1971, appellee's 17-year-old daughter was the victim of a rape and did not survive the incident. Six youths were soon indicted for murder and rape. Although there was substantial press coverage of the crime and of subsequent developments, the identity of the victim was not disclosed pending trial, perhaps because of Ga. Code Ann. s 26—9901 (1972),[1] which makes it a misdemeanor to publish or broadcast the name or identity of a rape victim. In April 1972, some eight months later, the six defendants appeared in court. Five pleaded guilty to rape or attempted rape, the charge of murder having been dropped. The guilty pleas were accepted by the court, and the trial of the defendant pleading not guilty was set for a later date.

In the course of the proceedings that day, appellant Wasell, a reporter covering the incident for his employer, learned the name of the victim from an examination of the indictments which were made available for his inspection in the courtroom. That the name of the victim appears in the indictments and that the indictments were public records available for inspection are not disputed. Later that day, Wassell broadcast over the facilities of station WSB—TV, a television station owned by appellant Cox Broadcasting Corp., a news report concerning the court proceedings. The report named the victim of the crime and was repeated the following day.

In May 1972, appellee brought an action for money damages against appellants, relying on s 26—9901 and claiming that his right to privacy had been invaded by the television broadcasts giving the name of his deceased daughter. Appellants admitted the broadcasts but claimed that they were privileged under both state law and the First and Fourteenth Amendments.

Georgia stoutly defends both s 26—9901 and the State's common-law privacy action challenged here. Its claims are not without force, for powerful arguments can be made, and have been made, that however it may be ultimately defined, there is a zone of privacy surrounding every individual, a zone within which the State may protect him from intrusion by the press, with all its attendant publicity. Indeed, the central thesis of the root article by Warren and Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890), was that the press was

---

[1] 'It shall be unlawful for any news media or any other person to print and publish, broadcast, televise, or disseminate through any other medium of public dissemination or cause to be printed and published, broadcast, televised, or disseminated in any newspaper, magazine, periodical or other publication published in this State or through any radio or television broadcast originating in the State the name or identity of any female who may have been raped or upon whom an assault with intent to commit rape may have been made. Any person or corporation violating the provisions of this section shall, upon conviction, be punished as for a misdemeanor.'

Three other States have similar statutes.

overstepping its prerogatives by publishing essentially private information and that there should be a remedy for the alleged abuses.

More compellingly, the century has experienced a strong tide running in favor of the so-called right of privacy. In 1967, we noted that "[i]t has been said that a 'right of privacy' has been recognized at common law in 30 States plus the District of Columbia and by statute in four States."

These are impressive credentials for a right of privacy, but we should recognize that we do not have at issue here an action for the invasion of privacy involving the appropriation of one's name or photograph, a physical or other tangible intrusion into a private area, or a publication of otherwise private information that is also false although perhaps not defamatory. The version of the privacy tort now before us—termed in Georgia "the tort of public disclosure,"—is that in which the plaintiff claims the right to be free from unwanted publicity about his private affairs, which, although wholly true, would be offensive to a person of ordinary sensibilities. Because the gravamen of the claimed injury is the publication of information, whether true or not, the dissemination of which is embarrassing or otherwise painful to an individual, it is here that claims of privacy most directly confront the constitutional freedoms of speech and press. The face-off is apparent, and the appellants urge upon us the broad holding that the press may not be made criminally or civilly liable for publishing information that is neither false nor misleading but absolutely accurate, however damaging it may be to reputation or individual sensibilities.

….Those precedents, as well as other considerations, counsel similar caution here. In this sphere of collision between claims of privacy and those of the free press, the interests on both sides are plainly rooted in the traditions and significant concerns of our society. Rather than address the broader question whether truthful publications may ever be subjected to civil or criminal liability consistently with the First and Fourteenth Amendments, or to put it another way, whether the State may ever define and protect an area of privacy free from unwanted publicity in the press, it is appropriate to focus on the narrower interface between press and privacy that this case presents, namely, whether the State may impose sanctions on the accurate publication of the name of a rape victim obtained from public records—more specifically, from judicial records which are maintained in connection with a public prosecution and which themselves are open to public inspection. We are convinced that the State may not do so.

In the first place, in a society in which each individual has but limited time and resources with which to observe at first hand the operations of his government, he relies necessarily upon the press to bring to him in convenient form the facts of those operations. Great responsibility is accordingly placed upon the news media to report fully and accurately the proceedings of government, and official records and documents open to the public are the basic data of governmental operations. Without the information provided by the press most of us and many of our representatives would be unable to vote intelligently or to register opinions on the administration of government generally. With respect to judicial proceedings in particular, the function of the press serves to guarantee the fairness of trials and to bring to bear the beneficial effects of public scrutiny upon the administration of justice.

Appellee has claimed in this litigation that the efforts of the press have infringed his right to privacy by broadcasting to the world the fact that his daughter was a rape victim. The commission of crime, prosecutions resulting from it, and judicial proceedings arising from the prosecutions, however, are without question events of legitimate concern to the public and consequently fall within the responsibility of the press to report the operations of government.

The special protected nature of accurate reports of judicial proceedings has repeatedly been recognized. This Court, in an opinion written by Mr. Justice Douglas, has said:

> "A trial is a public event. What transpires in the court room is public property. If a transcript of the court proceedings had been published, we suppose none would claim that the judge could punish the publisher for contempt. And we can see no difference though the conduct of the attorneys, of the jury, or even of the judge himself, may have reflected on the court. Those who see and hear what transpired can report it with impunity. There is no special perquisite of the judiciary which enables it, as distinguished from other institutions of democratic government, to suppress, edit, or censor events which transpire in proceedings before it." *Craig v. Harney*, 331 U.S. 367, 374 (1947).

The developing law surrounding the tort of invasion of privacy recognizes a privilege in the press to report the events of judicial proceedings. The Warren and Brandeis article noted that the proposed new right would be limited in the same manner as actions for libel and slander where such a publication was a privileged communication: "the right to privacy is not invaded by any publication made in a court of justice . . . and (at least in many jurisdictions) reports of any such proceedings would in some measure be accorded a like privilege."

The Restatement of Torts, s 867, embraced an action for privacy. [T]he commentary to s 652D states: "There is no liability when the defendant merely gives further publicity to information about the plaintiff which is already public. Thus there is no liability for giving publicity to facts about the plaintiff's life which are matters of public record." The same is true of the separate tort of physically or otherwise intruding upon the seclusion or private affairs of another. Section 652B, Comment c, provides that "there is no liability for the examination of a public record concerning the plaintiff, or of documents which the plaintiff is required to keep and make available for public inspection." According to this draft, ascertaining and publishing the contents of public records are simply not within the reach of these kinds of privacy actions.

Thus even the prevailing law of invasion of privacy generally recognizes that the interests in privacy fade when the information involved already appears on the public record. The conclusion is compelling when viewed in terms of the First and Fourteenth Amendments and in light of the public interest in a vigorous press.

By placing the information in the public domain on official court records, the State must be presumed to have concluded that the public interest was thereby being served. Public records by their very nature are of interest to those concerned with the administration of government, and a public benefit is performed by the reporting of the true contents of the records by the media. The freedom of the press to publish that information appears to us to be of critical importance to our type of government in which the citizenry is the final judge of the proper conduct of public business. In preserving that form of government the First and Fourteenth Amendments command nothing less than that the States may not impose sanctions on the publication of truthful information contained in official court records open to public inspection.

We are reluctant to embark on a course that would make public records generally available to the media but forbid their publication if offensive to the sensibilities of the supposed reasonable man. Such a rule would make it very difficult for the media to inform citizens about the public business and yet stay within the law. The rule would invite timidity and self-censorship and very likely lead to the suppression of many items that would otherwise be published and that should be made available to the public. At the very least, the First and Fourteenth Amendments will not allow exposing the press to liability for truthfully publishing information released to the public in official court records. If there are privacy interests to be protected in judicial proceedings, the States must respond by means which avoid public documentation or other exposure of private information. Their political institutions must weigh

the interests in privacy with the interests of the public to know and of the press to publish.[26] Once true information is disclosed in public court documents open to public inspection, the press cannot be sanctioned for publishing it. In this instance as in others reliance must rest upon the judgment of those who decide what to publish or broadcast.

Appellant Wassell based his televised report upon notes taken during the court proceedings and obtained the name of the victim from the indictments handed to him at his request during a recess in the hearing. Appellee has not contended that the name was obtained in an improper fashion or that it was not on an official court document open to public inspection. Under these circumstances, the protection of freedom of the press provided by the First and Fourteenth Amendments bars the State of Georgia from making appellants' broadcast the basis of civil liability.

Notes

1. One could view *Cox Broadcasting* through a very formulaic lens. Grant that the government has reason to protect the privacy of rape victims. Even given that, the government must do so in a sensible way. This way, which asks the reporters to keep secret information disclosed in open court, is not sensible. Is that a fair reading of the case? Is that a good way to understand the issue?
2. Notably, the plaintiff in the case is not the victim whose name is being disclosed, but instead her father. The dead do not generally have this form of privacy right, so the deceased victim's estate cannot sue and the father must proceed in his own name. To what extent does it make sense to recognize him as having a privacy right here? And, if he does have a right, would he still have one even were his daughter alive?

The Florida Star v. B.J.F., 491 U.S. 524 (1989)

Justice MARSHALL delivered the opinion of the Court.

Florida Stat. § 794.03 (1987) makes it unlawful to "print, publish, or broadcast . . . in any instrument of mass communication" the name of the victim of a sexual offense. Pursuant to this statute, appellant The Florida Star was found civilly liable for publishing the name of a rape victim which it had obtained from a publicly released police report. The issue presented here is whether this result comports with the First Amendment. We hold that it does not.

The Florida Star is a weekly newspaper which serves the community of Jacksonville, Florida, and which has an average circulation of approximately 18,000 copies. A regular feature of the newspaper is its "Police Reports" section. That section, typically two to three pages in length, contains brief articles describing local criminal incidents under police investigation.

On October 20, 1983, appellee B.J.F.[2] reported to the Duval County, Florida, Sheriff's Department (Department) that she had been robbed and sexually assaulted by an unknown assailant. The Department prepared a report on the incident which identified B.J.F. by her full name. The Department then placed the report in its pressroom. The Department does not restrict access either to the pressroom or to the reports made available therein.

A Florida Star reporter-trainee sent to the pressroom copied the police report verbatim, including B.J.F.'s full name, on a blank duplicate of the Department's forms. A Florida Star

---

[26] We mean to imply nothing about any constitutional questions which might arise from a state policy not allowing access by the public and press to various kinds of official records, such as records of juvenile-court proceedings.

[2] In filing this lawsuit, appellee used her full name in the caption of the case. On appeal, the Florida District Court of Appeal *sua sponte* revised the caption, stating that it would refer to the appellee by her initials, "in order to preserve [her] privacy interests." Respecting those interests, we, too, refer to appellee by her initials, both in the caption and in our discussion.

reporter then prepared a one-paragraph article about the crime, derived entirely from the trainee's copy of the police report. The article included B.J.F.'s full name. It appeared in the "Robberies" subsection of the "Police Reports" section on October 29, 1983, one of 54 police blotter stories in that day's edition. The article read:

"[B.J.F.] reported on Thursday, October 20, she was crossing Brentwood Park, which is in the 500 block of Golfair Boulevard, enroute to her bus stop, when an unknown black man ran up behind the lady and placed a knife to her neck and told her not to yell. The suspect then undressed the lady and had sexual intercourse with her before fleeing the scene with her 60 cents, Timex watch and gold necklace. Patrol efforts have been suspended concerning this incident because of a lack of evidence."

In printing B.J.F.'s full name, The Florida Star violated its internal policy of not publishing the names of sexual offense victims.

On September 26, 1984, B.J.F. filed suit in the Circuit Court of Duval County against the Department and The Florida Star, alleging that these parties negligently violated § 794.03. Before trial, the Department settled with B.J.F. for $2,500. The Florida Star moved to dismiss, claiming, *inter alia,* that imposing civil sanctions on the newspaper pursuant to § 794.03 violated the First Amendment. The trial judge rejected the motion.

At the ensuing daylong trial, B.J.F. testified that she had suffered emotional distress from the publication of her name. She stated that she had heard about the article from fellow workers and acquaintances; that her mother had received several threatening phone calls from a man who stated that he would rape B.J.F. again; and that these events had forced B.J.F. to change her phone number and residence, to seek police protection, and to obtain mental health counseling. In defense, The Florida Star put forth evidence indicating that the newspaper had learned B.J.F.'s name from the incident report released by the Department, and that the newspaper's violation of its internal rule against publishing the names of sexual offense victims was inadvertent.

At the close of B.J.F.'s case, and again at the close of its defense, The Florida Star moved for a directed verdict. On both occasions, the trial judge denied these motions.

The First District Court of Appeal affirmed in a three-paragraph *per curiam* opinion. In the paragraph devoted to The Florida Star's First Amendment claim, the court stated that the directed verdict for B.J.F. had been properly entered because, under § 794.03, a rape victim's name is "of a private nature and not to be published as a matter of law."

The Florida Star appealed to this Court. We noted probable jurisdiction . . . and now reverse.

The tension between the right which the First Amendment accords to a free press, on the one hand, and the protections which various statutes and common-law doctrines accord to personal privacy against the publication of truthful information, on the other, is a subject we have addressed several times in recent years. Our decisions in cases involving government attempts to sanction the accurate dissemination of information as invasive of privacy, have not, however, exhaustively considered this conflict. On the contrary, although our decisions have without exception upheld the press' right to publish, we have emphasized each time that we were resolving this conflict only as it arose in a discrete factual context.

The parties to this case frame their contentions in light of a trilogy of cases which have presented, in different contexts, the conflict between truthful reporting and state-protected privacy interests. In *Cox Broadcasting Corp. v. Cohn,* 420 U.S. 469 (1975), we found unconstitutional a civil damages award entered against a television station for broadcasting the name of a rape-murder victim which the station had obtained from courthouse records. In *Oklahoma Publishing Co. v. Oklahoma County District Court,* 430 U.S. 308 (1977), we found unconstitutional a state court's pretrial order enjoining the media from publishing the name or

photograph of an 11-year-old boy in connection with a juvenile proceeding involving that child which reporters had attended. Finally, in *Smith v. Daily Mail Publishing Co.,* 443 U.S. 97 (1979), we found unconstitutional the indictment of two newspapers for violating a state statute forbidding newspapers to publish, without written approval of the juvenile court, the name of any youth charged as a juvenile offender. The papers had learned about a shooting by monitoring a police band radio frequency and had obtained the name of the alleged juvenile assailant from witnesses, the police, and a local prosecutor.

Appellant takes the position that this case is indistinguishable from *Cox Broadcasting.* Alternatively, it urges that our decisions in the above trilogy, and in other cases in which we have held that the right of the press to publish truth overcame asserted interests other than personal privacy, can be distilled to yield a broader First Amendment principle that the press may never be punished, civilly or criminally, for publishing the truth.

We conclude that imposing damages on appellant for publishing B.J.F.'s name violates the First Amendment, although not for either of the reasons appellant urges. Despite the strong resemblance this case bears to *Cox Broadcasting,* that case cannot fairly be read as controlling here. The name of the rape victim in that case was obtained from courthouse records that were open to public inspection, a fact which Justice WHITE's opinion for the Court repeatedly noted. Significantly, one of the reasons we gave in *Cox Broadcasting* for invalidating the challenged damages award was the important role the press plays in subjecting trials to public scrutiny and thereby helping guarantee their fairness. That role is not directly compromised where, as here, the information in question comes from a police report prepared and disseminated at a time at which not only had no adversarial criminal proceedings begun, but no suspect had been identified.

Nor need we accept appellant's invitation to hold broadly that truthful publication may never be punished consistent with the First Amendment. Indeed, in *Cox Broadcasting,* we pointedly refused to answer even the less sweeping question "whether truthful publications may ever be subjected to civil or criminal liability" for invading "an area of privacy" defined by the State. Respecting the fact that press freedom and privacy rights are both "plainly rooted in the traditions and significant concerns of our society," we instead focused on the less sweeping issue "whether the State may impose sanctions on the accurate publication of the name of a rape victim obtained from public records—more specifically, from judicial records which are maintained in connection with a public prosecution and which themselves are open to public inspection." We continue to believe that the sensitivity and significance of the interests presented in clashes between First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case.

In our view, this case is appropriately analyzed with reference to such a limited First Amendment principle. It is the one, in fact, which we articulated in *Daily Mail* in our synthesis of prior cases involving attempts to punish truthful publication: "[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."

First, because the *Daily Mail* formulation only protects the publication of information which a newspaper has "lawfully obtain[ed]," . . . the government retains ample means of safeguarding significant interests upon which publication may impinge, including protecting a rape victim's anonymity. To the extent sensitive information rests in private hands, the government may under some circumstances forbid its nonconsensual acquisition, thereby bringing outside of the *Daily Mail* principle the publication of any information so acquired. To the extent sensitive information is in the government's custody, it has even greater power to forestall or mitigate the injury caused by its release. The government may classify certain information, establish and enforce procedures ensuring its redacted release, and extend a damages remedy against the government or its officials where the government's mishandling

of sensitive information leads to its dissemination. Where information is entrusted to the government, a less drastic means than punishing truthful publication almost always exists for guarding against the dissemination of private facts.[8]

A second consideration undergirding the *Daily Mail* principle is the fact that punishing the press for its dissemination of information which is already publicly available is relatively unlikely to advance the interests in the service of which the State seeks to act. It is not, of course, always the case that information lawfully acquired by the press is known, or accessible, to others. But where the government has made certain information publicly available, it is highly anomalous to sanction persons other than the source of its release. We noted this anomaly in *Cox Broadcasting:* "By placing the information in the public domain on official court records, the State must be presumed to have concluded that the public interest was thereby being served." The *Daily Mail* formulation reflects the fact that it is a limited set of cases indeed where, despite the accessibility of the public to certain information, a meaningful public interest is served by restricting its further release by other entities, like the press.

A third and final consideration is the "timidity and self-censorship" which may result from allowing the media to be punished for publishing certain truthful information. *Cox Broadcasting* noted this concern with overdeterrence in the context of information made public through official court records, but the fear of excessive media self-suppression is applicable as well to other information released, without qualification, by the government. A contrary rule, depriving protection to those who rely on the government's implied representations of the lawfulness of dissemination, would force upon the media the onerous obligation of sifting through government press releases, reports, and pronouncements to prune out material arguably unlawful for publication. This situation could inhere even where the newspaper's sole object was to reproduce, with no substantial change, the government's rendition of the event in question.

Applied to the instant case, the *Daily Mail* principle clearly commands reversal. The first inquiry is whether the newspaper "lawfully obtain[ed] truthful information about a matter of public significance." It is undisputed that the news article describing the assault on B.J.F. was accurate. In addition, appellant lawfully obtained B.J.F.'s name. Appellee's argument to the contrary is based on the fact that under Florida law, police reports which reveal the identity of the victim of a sexual offense are not among the matters of "public record" which the public, by law, is entitled to inspect. But the fact that state officials are not required to disclose such reports does not make it unlawful for a newspaper to receive them when furnished by the government. Nor does the fact that the Department apparently failed to fulfill its obligation under § 794.03 not to "cause or allow to be . . . published" the name of a sexual offense victim make the newspaper's ensuing receipt of this information unlawful. It is, clear, furthermore, that the news article concerned "a matter of public significance," . . . in the sense in which the *Daily Mail* synthesis of prior cases used that term. That is, the article generally, as opposed to the specific identity contained within it, involved a matter of paramount public import: the commission, and investigation, of a violent crime which had been reported to authorities.

The second inquiry is whether imposing liability on appellant pursuant to § 794.03 serves "a need to further a state interest of the highest order." Appellee argues that a rule punishing publication furthers three closely related interests: the privacy of victims of sexual offenses; the physical safety of such victims, who may be targeted for retaliation if their names become known to their assailants; and the goal of encouraging victims of such crimes to report these offenses without fear of exposure.

---

[8] The *Daily Mail* principle does not settle the issue whether, in cases where information has been acquired *unlawfully* by a newspaper or by a source, government may ever punish not only the unlawful acquisition, but the ensuing publication as well.

At a time in which we are daily reminded of the tragic reality of rape, it is undeniable that these are highly significant interests, a fact underscored by the Florida Legislature's explicit attempt to protect these interests by enacting a criminal statute prohibiting much dissemination of victim identities. We accordingly do not rule out the possibility that, in a proper case, imposing civil sanctions for publication of the name of a rape victim might be so overwhelmingly necessary to advance these interests as to satisfy the *Daily Mail* standard. For three independent reasons, however, imposing liability for publication under the circumstances of this case is too precipitous a means . . . .

First is the manner in which appellant obtained the identifying information in question. As we have noted, where the government itself provides information to the media, it is most appropriate to assume that the government had, but failed to utilize, far more limited means of guarding against dissemination than the extreme step of punishing truthful speech. Where, as here, the government has failed to police itself in disseminating information, it is clear . . . that the imposition of damages against the press for its subsequent publication can hardly be said to be a narrowly tailored means of safeguarding anonymity. Once the government has placed such information in the public domain, "reliance must rest upon the judgment of those who decide what to publish or broadcast," *Cox Broadcasting,* and hopes for restitution must rest upon the willingness of the government to compensate victims for their loss of privacy and to protect them from the other consequences of its mishandling of the information which these victims provided in confidence.

That appellant gained access to the information in question through a government news release makes it especially likely that, if liability were to be imposed, self-censorship would result. Reliance on a news release is a paradigmatically "routine newspaper reporting techniqu[e]." *Daily Mail*. The government's issuance of such a release, without qualification, can only convey to recipients that the government considered dissemination lawful, and indeed expected the recipients to disseminate the information further. Had appellant merely reproduced the news release prepared and released by the Department, imposing civil damages would surely violate the First Amendment. The fact that appellant converted the police report into a news story by adding the linguistic connecting tissue necessary to transform the report's facts into full sentences cannot change this result.

A second problem with Florida's imposition of liability for publication is the broad sweep of the negligence *per se* standard applied under the civil cause of action implied from § 794.03. Unlike claims based on the common law tort of invasion of privacy, . . . civil actions based on § 794.03 require no case-by-case findings that the disclosure of a fact about a person's private life was one that a reasonable person would find highly offensive. On the contrary, under the *per se* theory of negligence adopted by the courts below, liability follows automatically from publication. This is so regardless of whether the identity of the victim is already known throughout the community; whether the victim has voluntarily called public attention to the offense; or whether the identity of the victim has otherwise become a reasonable subject of public concern—because, perhaps, questions have arisen whether the victim fabricated an assault by a particular person. Nor is there a scienter requirement of any kind under § 794.03, engendering the perverse result that truthful publications challenged pursuant to this cause of action are less protected by the First Amendment than even the least protected defamatory falsehoods: those involving purely private figures, where liability is evaluated under a standard, usually applied by a jury, of ordinary negligence.

Third, and finally, the facial underinclusiveness of § 794.03 raises serious doubts about whether Florida is, in fact, serving, with this statute, the significant interests which appellee invokes in support of affirmance. Section 794.03 prohibits the publication of identifying information only if this information appears in an "instrument of mass communication," a term the statute does not define. Section 794.03 does not prohibit the spread by other means of the identities of victims of sexual offenses. An individual who maliciously spreads word of the

identity of a rape victim is thus not covered, despite the fact that the communication of such information to persons who live near, or work with, the victim may have consequences as devastating as the exposure of her name to large numbers of strangers.

When a State attempts the extraordinary measure of punishing truthful publication in the name of privacy, it must demonstrate its commitment to advancing this interest by applying its prohibition evenhandedly, to the smalltime disseminator as well as the media giant. Where important First Amendment interests are at stake, the mass scope of disclosure is not an acceptable surrogate for injury. Without more careful and inclusive precautions against alternative forms of dissemination, we cannot conclude that Florida's selective ban on publication by the mass media satisfactorily accomplishes its stated purpose.

Our holding today is limited. We do not hold that truthful publication is automatically constitutionally protected, or that there is no zone of personal privacy within which the State may protect the individual from intrusion by the press, or even that a State may never punish publication of the name of a victim of a sexual offense. We hold only that where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order, and that no such interest is satisfactorily served by imposing liability under § 794.03 to appellant under the facts of this case. The decision below is therefore *reversed*.

Justice WHITE, with whom THE CHIEF JUSTICE and Justice O'CONNOR join, dissenting.

"Short of homicide, [rape] is the 'ultimate violation of self.'" *Coker v. Georgia,* 433 U.S. 584, 597 (1977) (opinion of WHITE, J.). For B.J.F., however, the violation she suffered at a rapist's knifepoint marked only the beginning of her ordeal. A week later, while her assailant was still at large, an account of this assault—identifying by name B.J.F. as the victim—was published by The Florida Star. As a result, B.J.F. received harassing phone calls, required mental health counseling, was forced to move from her home, and was even threatened with being raped again. Yet today, the Court holds that a jury award of $75,000 to compensate B.J.F. for the harm she suffered due to the Star's negligence is at odds with the First Amendment. I do not accept this result.

Cox Broadcasting reversed a damages award entered against a television station, which had obtained a rape victim's name from public records maintained in connection with the judicial proceedings brought against her assailants. While there are similarities, critical aspects of that case make it wholly distinguishable from this one. First, in *Cox Broadcasting,* the victim's name had been disclosed in the hearing where her assailants pleaded guilty; and, as we recognized, judicial records have always been considered public information in this country. Second, unlike the incident report at issue here, which was meant by state law to be withheld from public release, the judicial proceedings at issue in *Cox Broadcasting* were open as a matter of state law. Thus, in *Cox Broadcasting,* the state-law scheme made public disclosure of the victim's name almost inevitable; here, Florida law forbids such disclosure.

Cox Broadcasting stands for the proposition that the State cannot make the press its first line of defense in withholding private information from the public—it cannot ask the press to secrete private facts that the State makes no effort to safeguard in the first place. In this case, however, the State has undertaken "means which avoid [but obviously, not altogether prevent] public documentation or other exposure of private information."

Finding *Cox Broadcasting* inadequate to support its result, the Court relies on *Smith v. Daily Mail Publishing Co.* as its principal authority. But the flat rule from *Daily Mail* on which the Court places so much reliance—"[I]f a newspaper lawfully obtains truthful information . . . then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order"—was introduced in *Daily Mail* with the cautious qualifier that such a rule was "suggest[ed]" by our prior cases, "[n]one of [which] . . .

directly control[led]" in *Daily Mail.* The rule the Court takes as a given was thus offered only as a hypothesis in *Daily Mail:* it should not be so uncritically accepted as constitutional dogma.

We are left, then, to wonder whether the three "independent reasons" the Court cites for reversing the judgment for B.J.F. support its result.

The first of these reasons relied on by the Court is the fact "appellant gained access to [B.J.F.'s name] through a government news release." "The government's issuance of such a release, without qualification, can only convey to recipients that the government considered dissemination lawful," the Court suggests. So described, this case begins to look like the situation in *Oklahoma Publishing,* where a judge invited reporters into his courtroom, but then tried to prohibit them from reporting on the proceedings they observed. But this case is profoundly different. Here, the "release" of information provided by the government was not, as the Court says, "without qualification." As the Star's own reporter conceded at trial, the crime incident report that inadvertently included B.J.F.'s name was posted in a room that contained signs making it clear that the names of rape victims were not matters of public record, and were not to be published. The Star's reporter indicated that she understood that she "[was not] allowed to take down that information" (*i.e.,* B.J.F.'s name) and that she "[was] not supposed to take the information from the police department." Thus, by her own admission the posting of the incident report did not convey to the Star's reporter the idea that "the government considered dissemination lawful"; the Court's suggestion to the contrary is inapt.

Instead, Florida has done precisely what we suggested, in *Cox Broadcasting,* that States wishing to protect the privacy rights of rape victims might do: "respond [to the challenge] by means which *avoid* public documentation or other exposure of private information." By amending its public records statute to exempt rape victims' names from disclosure . . . and forbidding its officials to release such information, . . . the State has taken virtually every step imaginable to prevent what happened here. This case presents a far cry, then, from *Cox Broadcasting* or *Oklahoma Publishing,* where the State asked the news media not to publish information it had made generally available to the public: here, the State is not asking the media to do the State's job in the first instance. Unfortunately, as this case illustrates, mistakes happen: even when States take measures to "avoid" disclosure, sometimes rape victims' names are found out. As I see it, it is not too much to ask the press, in instances such as this, to respect simple standards of decency and refrain from publishing a victims' name, address, and/or phone number.[2]

Second, the Court complains that appellant was judged here under too strict a liability standard. The Court contends that a newspaper might be found liable under the Florida courts' negligence *per se* theory without regard to a newspaper's scienter or degree of fault. The short answer to this complaint is that whatever merit the Court's argument might have, it is wholly inapposite here, where the jury found that appellant acted with "reckless indifference towards the rights of others[.]" . . . .

Third, the Court faults the Florida criminal statute for being underinclusive: § 794.03 covers disclosure of rape victims' names in "instrument[s] of mass communication," but not other means of distribution, the Court observes. But our cases which have struck down laws that limit or burden the press due to their underinclusiveness have involved situations where a legislature has singled out one segment of the news media or press for adverse treatment, see, *e.g., Daily Mail* (restricting newspapers and not radio or television), or singled out the press for adverse treatment when compared to other similarly situated enterprises . . . . Here, the Florida law evenhandedly covers all "instrument[s] of mass communication" no matter their form, media, content, nature, or purpose. It excludes neighborhood gossips . . . because presumably

[2] The Court's concern for a free press is appropriate, but such concerns should be balanced against rival interests in a civilized and humane society. An absolutist view of the former leads to insensitivity as to the latter.

the Florida Legislature has determined that neighborhood gossips do not pose the danger and intrusion to rape victims that "instrument[s] of mass communication" do. Simply put: Florida wanted to prevent the widespread distribution of rape victims' names, and therefore enacted a statute tailored almost as precisely as possible to achieving that end.

Moreover, the Court's "underinclusiveness" analysis itself is "underinclusive." After all, the lawsuit against the Star which is at issue here is not an action for violating the statute which the Court deems underinclusive, but is, more accurately, for the negligent publication of appellee's name. The scheme which the Court should review, then, is not only § 794.03 (which, as noted above, merely provided the standard of care in this litigation), but rather, the whole of Florida privacy tort law. As to the latter, Florida does recognize a tort of publication of private facts. Thus, it is quite possible that the neighborhood gossip whom the Court so fears being left scot free to spread news of a rape victim's identity would be subjected to the same (or similar) liability regime under which appellant was taxed. The Court's myopic focus on § 794.03 ignores the probability that Florida law is more comprehensive than the Court gives it credit for being.

At issue in this case is whether there is any information about people, which—though true—may not be published in the press. By holding that only "a state interest of the highest order" permits the State to penalize the publication of truthful information, and by holding that protecting a rape victim's right to privacy is not among those state interests of the highest order, the Court accepts appellant's invitation . . . to obliterate one of the most noteworthy legal inventions of the 20th century: the tort of the publication of private facts. Even if the Court's opinion does not say as much today, such obliteration will follow inevitably from the Court's conclusion here. If the First Amendment prohibits wholly private persons (such as B.J.F.) from recovering for the publication of the fact that she was raped, I doubt that there remain any "private facts" which persons may assume will not be published in the newspapers or broadcast on television.

Notes

1. *Florida Star* explains the circumstances under which the publication of truthful private facts might be punished. Such publication may be sanctioned in one of three circumstances:
    a. The information was not lawfully obtained, or
    b. The information is not "about a matter of public significance," or
    c. Sanctioning the publication is the least restrictive means to further a state interest of the highest order.

    The majority then appears to hold that the remedy in *Florida Star* does not satisfy the third test, because the remedy is not narrowly tailored to promote an interest that apparently is of the highest order.
2. The Court's analysis in the case may fail to recognize the dynamic nature of this problem. The amount of information the government provides to the press may change depending on the legal rule that governs how the press is allowed to use it. Imagine two regimes. In regime one, the government may admit the press to a courtroom or battlefield and then restrict what reporters can publish to protect privacy or military secrets. In regime two, the government must permit the press to speak without restrictions, but is not compelled to admit reporters to a courtroom or battlefield in the first place. In a world governed by regime two, the press is more free to speak, but more likely to be denied access to critical events. This still may be the better rule, but there is a tradeoff that the court appears to neglect. One would imagine that the natural reaction to *Florida Star* is to cease giving the press easy access to fresh police reports.

Publius v. Boyer–Vine, 237 F.Supp.3d 997 (E.D. Cal. 2017)

Lawrence J. O'Neill, UNITED STATES CHIEF DISTRICT JUDGE

On July 1, 2016, California Governor Jerry Brown signed several gun control bills into law. One of those bills established a database tracking all ammunition purchases in California. The database includes the driver's license information, residential address and telephone number, and date of birth for anyone who purchases or transfers ammunition in California.

Publius maintains a political blog under the name, "The Real Write Winger." On July 5, 2016, in response to the California legislature's gun control legislation, he posted the following blog entry, titled "Tyrants to be registered with California gun owners":

> If you're a gun owner in California, the government knows where you live. With the recent anti gun, anti Liberty bills passed by the legisexuals in the State Capitol and signed into law by our senile communist governor, isn't it about time to register these tyrants with gun owners?
>
> Compiled below is the names, home addresses, and home phone numbers of all the legislators who decided to make you a criminal if you don't abide by their dictates. "Isn't that dangerous, what if something bad happens to them by making that information public?" First, all this information was already public; it's just now in one convenient location. Second, it's no more dangerous than, say, these tyrants making it possible for free men and women to have government guns pointed at them while they're hauled away to jail and prosecuted for the crime of exercising their rights and Liberty.
>
> These tyrants are no longer going to be insulated from us. They used their power we entrusted them with to exercise violence against us if we don't give up our rights and Liberty. This common sense tyrant registration addresses this public safety hazard by giving the public the knowledge of who and where these tyrants are in case they wish to use their power for violence again.
>
> So below is the current tyrant registry. These are the people who voted to send you to prison if you exercise your rights and liberties. This will be a constantly updated list depending on future votes, and if you see a missing address or one that needs updating, please feel free to contact me. And please share this with every California gun owner you know.
>
> To be fair, the only way for a tyrant to have their name removed from the tyrant registry is to pass laws which repeal the laws that got them added to the list, or upon the tyrant's death. Otherwise, it is a permanent list, even after the tyrant leaves office. The people will retain this information and have access to it indefinitely.

Through searching public records for free on zabasearch.com,[2] Publius compiled the names, home addresses, and phone numbers of 40 California legislature members who had voted in favor of the gun control measures. He then posted that information on his blog.

---

[2] Defendant describes Zabasearch as "a commercial vendor," and therefore contends Publius "did not obtain the legislators' addresses from public records." But, according to zabasearch.com, "[a]ll information found using ZabaSearch comes from public records databases. That means information collected by the government, such as court records, country records, state records, such as the kind of information that becomes public when you buy a new house or file a change-of-address form with the United States Postal Service." See www.zabasearch.com/faq (last visited February 7, 2017). Defendant therefore does not dispute that the legislators' personal information Publius posted was publicly available.

In the days that followed, several legislators received threatening phone calls and social media messages that appeared to have been prompted by Publius's blog entry. Specifically,

> there were reports from at least four different State Senators that either they or one of their family members had received a phone call at their residence from an unidentified male speaker saying, "I know your address and don't you wish you knew who I am?" One of the calls was received by the step-son of a Senator who was alone in the home while the Senator and his wife were away. At least two other Senators had reported receiving (and forwarded to the [California Senate] Sergeant-at-Arms) threatening social media messages; one warned: "You have no right to pass laws to take my constitutional rights away. (2nd & 1st amendments) Let alone pass a bill that makes you exempt from the very same laws. I've have [sic] shared your home address in the Internet. The People will be acting on this."

The Senate Sergeant-at-Arms sent the Office "a request to seek the removal of the legislators' home addresses from the internet pursuant to section 6254.21(c)." In response, on July 8, 2016, Deputy Legislative Counsel Kathryn Londenberg sent a written demand to WordPress.com, who hosted Plaintiff's blog. WordPress immediately removed Publius's entire blog entry.

Plaintiffs contend § 6254.21(c) is a content-based restriction on constitutionally protected speech that violates the First Amendment on its face and as applied to them. Defendant does not dispute the statute is content-based, but argues it is nonetheless lawful under the First Amendment.

As to Plaintiffs' facial challenge, they contend § 6254.21(c) is impermissibly overbroad. "[A] law may be invalidated as overbroad if 'a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep.' " But "because a successful overbreadth challenge renders a statute unconstitutional and, therefore, invalid in *all* its applications ... the doctrine is employed sparingly and only as a last resort." Accordingly, when a litigant brings both an as-applied and facial challenge, the Supreme Court has strongly suggested that courts should address the facial challenge only if the as-applied challenge fails. *See Serafine v. Branaman*, 810 F.3d 354, 363 n.19 (5th Cir. 2016) (collecting cases). The Court therefore turns first to Plaintiffs' as-applied challenge.

Section § 6254.21(c)(1)(A) prohibits anyone from posting or displaying the home address or telephone number of certain government officials, if the official makes "a written demand" that his or her personal information not be displayed. The written demand must "include a statement describing a threat or fear for the safety of that official or of any person residing at the official's home address." A written demand is "effective for four years." After receiving such a written demand, the recipient must remove the official's home address and/or phone number from the internet within 48 hours, and may not "transfer" it to anyone through any medium.

"An official whose home address or telephone number is made public as a result of a violation of [§ 6254.21(c)(1)] may bring an action seeking injunctive or declarative relief." § 6254.21(c)(2). "If a court finds that a violation has occurred, it may grant injunctive or declarative relief and shall award the official court costs and reasonable attorney's fees."

An enforcing official could not determine whether § 6254.21(c)(1) applies to particular speech without determining if (1) the speech contains a home address and/or phone number of (2) a covered official. The statute is therefore content-based on its face: it applies only to speech that contains certain content—the "home address or telephone number of any elected or appointed [California] official." *See Reed v. Town of Gilbert, Ariz* (2015) ("Government regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed." *see also S.O.C., Inc. v. Cty. of Clark* (9th Cir. 1998) (holding that regulations that require officials to examine content of speech to determine whether regulation applies are content-based (collecting cases)).

"Content-based laws—those that target speech based on its communicative content—are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests." This requires the government to show that the law is "the least restrictive means to further a compelling interest."

"As a general matter, 'state action to punish the publication of truthful information seldom can satisfy constitutional standards.' " *Bartnicki v. Vopper* (2001). "More specifically, [the Supreme Court] has repeatedly held that 'if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need ... of the highest order.' "

Defendant suggests, in a footnote, that it is "questionable" whether the legislators' personal information is "a matter of public significance." For decades, the Supreme Court has broadly held that "[p]ublic records by their very nature are of interest to those connected with the administration of government, and a public benefit is performed by the reporting of the true contents of the records by the media." *Cox Broadcasting Corp. v. Cohn* (1975). Thus, several cases demonstrate that the First Amendment protects the right to publish highly personal information of private individuals, such as the names of rape victims and juveniles involved in legal proceedings, when they relate to matters of public concern.

Viewed in isolation, the legislators' home address and phone numbers may not, in and of themselves, constitute "a matter of public significance." But when considered in the specific context of Plaintiffs' speech—political protest, which is "core political speech," with First Amendment protection "at its zenith."—the information takes on new meaning. Publius searched publicly available documents and compiled the legislators' personal information specifically in response to legislation that required the government to maintain a database with the personal information of individuals who buy firearms and ammunition in California. When viewed in that context of political speech, the legislators' personal information becomes a matter of public concern.

…*Ostergren*, 615 F.3d 263, a case Plaintiffs characterize as "closely analogous" to this one, is particularly illustrative here. In that case, the plaintiff brought an as-applied challenge to a Virginia statute that prohibited "[i]ntentionally communicat[ing] another individual's social security number ("SSN") to the general public." "Calling attention to Virginia's practice of placing land records on the Internet without first redacting SSNs, [the plaintiff] displayed copies of Virginia land records containing unredacted SSNs on her website." By doing so, she sought "to publicize her message that governments are mishandling SSNs and generate pressure for reform." The information the plaintiff posted on her website was publicly available for a nominal fee, but her website made the public records "more accessible to the public than they [we]re through Virginia's [records] system."

Before she could be prosecuted for posting the SSNs on her website, the plaintiff challenged the Virginia statute as applied to her website on First Amendment grounds. As a threshold matter, the Fourth Circuit rejected the government's position that unredacted SSNs are entirely unprotected speech under the First Amendment. The court reasoned that, in the plaintiff's case, the unredacted SSNs "are integral to her message," and, in fact, "they *are* her message" because her "[d]isplaying them proves Virginia's failure to safeguard private information and powerfully demonstrates why Virginia citizens should be concerned." Although the plaintiff could have redacted the SSNs, the First Amendment protected the plaintiff's "freedom to decide how her message should be communicated." The Fourth Circuit therefore concluded that the plaintiff's speech "plainly concern[ed] a matter of public significance ... because displaying the contents of public records and criticizing Virginia's release of private information convey political messages that concern the public, *see Cox Broad.* ('Public records by their very nature are of interest to those concerned with the administration of government, and a public benefit is performed by the reporting of the true contents of the records by the media.')."

Florida Star, *Brayshaw*, *Sheehan*, and *Ostergren* thus show that highly personal information has public significance when inextricably associated with political speech. That principle applies here. Plaintiffs oppose, among other things, California legislation that requires the creation and maintenance of a database run by the California Department of Justice that compiles the residential address and telephone number of anyone who purchases or transfers firearms ammunition in California. Plaintiffs' means of protesting the legislation is by compiling their own "database" of the legislators' residential addresses and phone numbers. Like the plaintiff in *Ostergren*, that information is not just "integral to [Plaintiffs'] message," it *is* their message.

There is no dispute that Plaintiffs lawfully obtained and truthfully published information that was readily available online. When lawfully obtained, the truthful publication of that information falls within the First Amendment's ambit.... Specifically, if an individual publishes lawfully obtained, "truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need ... of the highest order." *Daily Mail*. Any law that seeks to meet that need must be narrowly tailored. *Florida Star*.

The Court assumes that the interest underlying § 6254.21(c)—protecting the personal safety of covered officials and their families—is a state interest of the highest order. But the Court need not decide whether it is because the statute is not narrowly tailored to further that interest.

First, § 6254.21(c) makes no attempt to prohibit or prevent true threats. Under the statute, a covered official need only subjectively fear for his or her safety (or that of his or her family) due to his or her home address or telephone number being online. To make a compliant request that the information be removed, the official need only send the publisher of the information a "statement describing a threat or fear for the safety of that official or of any person residing at the official's home address." If the official does so, the recipient must comply or face a lawsuit. An official can therefore make an effective takedown demand by informing someone who has posted the official's home address or phone number that doing so has made the official fear for his or her safety. On its face, § 6254.21(c)(1) does not require that the threat be credible or that a third-party review whether the official's request is well-founded. The statute makes no distinction between those who publish a covered official's home address or phone number online for wholly lawful reasons and those who do so for wholly unlawful reasons. So long as an official subjectively feels threatened, the official may make a takedown request. And if the publisher fails to comply with an official's takedown request within 48 hours, then he or she has violated § 6254.21(c)(1), which will entitle the official to bring suit in which attorney's fees would be awarded automatically to the official. This lack of case-by-case oversight and effective *per se* liability suggests that § 6254.21(c) is not narrowly tailored.

Section § 6254.21(c)(1) is not narrowly tailored for the additional reason that it does not differentiate between acts that "make public" previously private information and those that "make public" information that is already publicly available. There is no dispute that the information Publius compiled and posted, and a member of Hoskins's forum re-posted, was publicly available and readily accessible online. "[P]unishing [Plaintiffs] for [their] dissemination of information which is already publicly available is relatively unlikely to advance the interests in the service of which the State seeks to act." *Florida Star*. When "the government has failed to police itself in disseminating information, it is clear ... that the imposition of damages against the press for its subsequent publication can hardly be said to be a narrowly tailored means" to further the state's interests. Because the information Plaintiffs published came from freely available public records, § 6252.21(c)(1) is not narrowly tailored to protecting the safety of covered officials and their families.

Third, § 6254.21(c)(1) is underinclusive. A statute is underinclusive when it affects "too little speech," such that there are "doubts about whether the government is in fact pursuing the

interest it invokes, rather than disfavoring a particular speaker or viewpoint." …It proscribes the dissemination of a covered official's home address and phone number only on the internet, regardless of the extent to which it is available or disseminated elsewhere. That the statute does not prohibit a major newspaper or television channel from publishing the information, but would potentially prohibit an online blog with a limited audience from doing so, raises serious questions about whether it is serving its intended goals.

The Court therefore concludes § 6254.21(c)(1) is not narrowly tailored to serve its underlying interests. As noted above, the statute could be less restrictive in that it could proscribe only true threats, or it could require a neutral third-party to determine if the official's fear is objectively sound, or it could permit an objective case-by-case determination for liability instead of permitting a covered official to trigger its protections due to the official's subjective concerns. In summary, the Court finds that Plaintiffs are likely to succeed on their claim that § 6254.21(c)(1) is unconstitutional as applied to them.

Notes

1. The California statute here is an early example of a state anti-doxing statute, meaning a statute that prohibits distributing the personal information (usually address, telephone number, or other location or contact information) of an individual if done with sufficiently dangerous *mens rea*. For example, the relevant Illinois statute prohibits a person from publishing another's personally identifiable information if:

   > the information is published with the intent that it be used to harm or harass the person whose information is published and with knowledge or reckless disregard that the person whose information is published would be reasonably likely to suffer death, bodily injury, or stalking; and [the publication causes significant economic injury, emotional distress, fear of serious bodily injury, or substantial life disruption].

   740 ILCS 195/10. The act includes exceptions for reporting criminal activity and for doing so in connection with activity protected by the freedom of speech, the press, or similar. It is also permissible to provide "personally identifiable information to the press." If *Publius* is correctly decided, is the Illinois statute constitutional? It provides a civil cause of action and allows for the award of attorney fees to the plaintiff at the court's discretion and to the defendant if "the court finds [the action] was frivolous, baseless, or brought in bad faith."

Bartnicki v. Vopper, 532 U.S. 514 (2001)

Justice STEVENS delivered the opinion of the Court.

These cases raise an important question concerning what degree of protection, if any, the First Amendment provides to speech that discloses the contents of an illegally intercepted communication. That question is both novel and narrow. Despite the fact that federal law has prohibited such disclosures since 1934, this is the first time that we have confronted such an issue.

The suit at hand involves the repeated intentional disclosure of an illegally intercepted cellular telephone conversation about a public issue.

During 1992 and most of 1993, the Pennsylvania State Education Association, a union representing the teachers at the Wyoming Valley West High School, engaged in collective-bargaining negotiations with the school board. Petitioner Kane, then the president of the local union, testified that the negotiations were " 'contentious' " and received "a lot of media attention." In May 1993, petitioner Bartnicki, who was acting as the union's "chief negotiator," used the cellular phone in her car to call Kane and engage in a lengthy conversation about the status of the negotiations. An unidentified person intercepted and recorded that call.

In their conversation, Kane and Bartnicki discussed the timing of a proposed strike, difficulties created by public comment on the negotiations, and the need for a dramatic response to the board's intransigence. At one point, Kane said: " 'If they're not gonna move for three percent, we're gonna have to go to their, their homes .... To blow off their front porches, we'll have to do some work on some of those guys. (PAUSES). Really, uh, really and truthfully because this is, you know, this is bad news. (UNDECIPHERABLE).' "

In the early fall of 1993, the parties accepted a nonbinding arbitration proposal that was generally favorable to the teachers. In connection with news reports about the settlement, respondent Vopper, a radio commentator who had been critical of the union in the past, played a tape of the intercepted conversation on his public affairs talk show. Another station also broadcast the tape, and local newspapers published its contents. After filing suit against Vopper and other representatives of the media, Bartnicki and Kane (hereinafter petitioners) learned through discovery that Vopper had obtained the tape from respondent Jack Yocum, the head of a local taxpayers' organization that had opposed the union's demands throughout the negotiations. Yocum, who was added as a defendant, testified that he had found the tape in his mailbox shortly after the interception and recognized the voices of Bartnicki and Kane. Yocum played the tape for some members of the school board, and later delivered the tape itself to Vopper.

In their amended complaint, petitioners alleged that their telephone conversation had been surreptitiously intercepted by an unknown person using an electronic device, that Yocum had obtained a tape of that conversation, and that he intentionally disclosed it to Vopper, as well as other individuals and media representatives. Thereafter, Vopper and other members of the media repeatedly published the contents of that conversation. The amended complaint alleged that each of the defendants "knew or had reason to know" that the recording of the private telephone conversation had been obtained by means of an illegal interception. Relying on both federal and Pennsylvania statutory provisions, petitioners sought actual damages, statutory damages, punitive damages, and attorney's fees and costs.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 211, entitled Wiretapping and Electronic Surveillance [has the stated purpose] "to protect effectively the privacy of wire and oral communications." In addition to authorizing and regulating electronic surveillance for law enforcement purposes, Title III also regulated private conduct. One part of those regulations, § 2511(1), defined five offenses punishable by a fine of not more than $10,000, by imprisonment for not more than five years, or by both. Subsection (a) applied to any person who "willfully intercepts ... any wire or oral communication." Subsection (b) applied to the intentional use of devices designed to intercept oral conversations; subsection (d) applied to the use of the contents of illegally intercepted wire or oral communications; and subsection (e) prohibited the unauthorized disclosure of the contents of interceptions that were authorized for law enforcement purposes. Subsection (c), the original version of the provision most directly at issue in this suit, applied to any person who "willfully discloses, or endeavors to disclose, to any other person the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection." The oral communications protected by the Act were only those "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." § 2510(2).

The constitutional question before us concerns the validity of the statutes as applied to the specific facts of these cases. Because of the procedural posture of these cases, it is appropriate to make certain important assumptions about those facts. We accept petitioners' submission that the interception was intentional, and therefore unlawful, and that, at a minimum, respondents "had reason to know" that it was unlawful. Accordingly, the disclosure of the contents of the intercepted conversation by Yocum to school board members and to representatives of the media, as well as the subsequent disclosures by the media defendants to

the public, violated the federal and state statutes. The only question is whether the application of these statutes in such circumstances violates the First Amendment.

In answering that question, we accept respondents' submission on three factual matters that serve to distinguish most of the cases that have arisen under § 2511. First, respondents played no part in the illegal interception. Rather, they found out about the interception only after it occurred, and in fact never learned the identity of the person or persons who made the interception. Second, their access to the information on the tapes was obtained lawfully, even though the information itself was intercepted unlawfully by someone else. Third, the subject matter of the conversation was a matter of public concern. If the statements about the labor negotiations had been made in a public arena—during a bargaining session, for example—they would have been newsworthy. This would also be true if a third party had inadvertently overheard Bartnicki making the same statements to Kane when the two thought they were alone.

We agree with petitioners that § 2511(1)(c), as well as its Pennsylvania analog, is in fact a content-neutral law of general applicability. In determining whether a regulation is content based or content neutral, we look to the purpose behind the regulation; typically, "[g]overnment regulation of expressive activity is content neutral so long as it is '*justified* without reference to the content of the regulated speech.' "

The statute does not distinguish based on the content of the intercepted conversations, nor is it justified by reference to the content of those conversations. Rather, the communications at issue are singled out by virtue of the fact that they were illegally intercepted—by virtue of the source, rather than the subject matter. On the other hand, the naked prohibition against disclosures is fairly characterized as a regulation of pure speech.

As a general matter, "state action to punish the publication of truthful information seldom can satisfy constitutional standards." *Smith v. Daily Mail Publishing*, 443 U.S. 97, 102 (1979). More specifically, this Court has repeatedly held that "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need ... of the highest order."

However, *New York Times v. United States* raised, but did not resolve, the question "whether, in cases where information has been acquired *unlawfully* by a newspaper or by a source, government may ever punish not only the unlawful acquisition, but the ensuing publication as well." *Florida Star,* 491 U.S. at 535, n. 8. The question here, however, is a narrower version of that still-open question. Simply put, the issue here is this: "Where the punished publisher of information has obtained the information in question in a manner lawful in itself but from a source who has obtained it unlawfully, may the government punish the ensuing publication of that information based on the defect in a chain?" *Boehner,* 191 F.3d at 484–485 (Sentelle, J., dissenting).

The Government identifies two interests served by the statute—first, the interest in removing an incentive for parties to intercept private conversations, and second, the interest in minimizing the harm to persons whose conversations have been illegally intercepted. We assume that those interests adequately justify the prohibition in § 2511(1)(d) against the interceptor's own use of information that he or she acquired by violating § 2511(1)(a), but it by no means follows that punishing disclosures of lawfully obtained information of public interest by one not involved in the initial illegality is an acceptable means of serving those ends.

The normal method of deterring unlawful conduct is to impose an appropriate punishment on the person who engages in it. If the sanctions that presently attach to a violation of § 2511(1)(a) do not provide sufficient deterrence, perhaps those sanctions should be made more severe. But it would be quite remarkable to hold that speech by a law-abiding possessor of information can be suppressed in order to deter conduct by a non-law-abiding third party.

Although there are some rare occasions in which a law suppressing one party's speech may be justified by an interest in deterring criminal conduct by another, . . . this is not such a case.

With only a handful of exceptions, the violations of § 2511(1)(a) that have been described in litigated cases have been motivated by either financial gain or domestic disputes. In virtually all of those cases, the identity of the person or persons intercepting the communication has been known. Moreover, petitioners cite no evidence that Congress viewed the prohibition against disclosures as a response to the difficulty of identifying persons making improper use of scanners and other surveillance devices and accordingly of deterring such conduct, and there is no empirical evidence to support the assumption that the prohibition against disclosures reduces the number of illegal interceptions.

Although this suit demonstrates that there may be an occasional situation in which an anonymous scanner will risk criminal prosecution by passing on information without any expectation of financial reward or public praise, surely this is the exceptional case. Moreover, there is no basis for assuming that imposing sanctions upon respondents will deter the unidentified scanner from continuing to engage in surreptitious interceptions.

The Government's second argument, however, is considerably stronger. Privacy of communication is an important interest . . . and Title III's restrictions are intended to protect that interest, thereby "encouraging the uninhibited exchange of ideas and information among private parties...." Moreover, the fear of public disclosure of private conversations might well have a chilling effect on private speech.

Accordingly, it seems to us that there are important interests to be considered on *both* sides of the constitutional calculus. In considering that balance, we acknowledge that some intrusions on privacy are more offensive than others, and that the disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself. As a result, there is a valid independent justification for prohibiting such disclosures by persons who lawfully obtained access to the contents of an illegally intercepted message, even if that prohibition does not play a significant role in preventing such interceptions from occurring in the first place.

We need not decide whether that interest is strong enough to justify the application of § 2511(c) to disclosures of trade secrets or domestic gossip or other information of purely private concern. In other words, the outcome of these cases does not turn on whether § 2511(1)(c) may be enforced with respect to most violations of the statute without offending the First Amendment. The enforcement of that provision in these cases, however, implicates the core purposes of the First Amendment because it imposes sanctions on the publication of truthful information of public concern.

In these cases, privacy concerns give way when balanced against the interest in publishing matters of public importance. As Warren and Brandeis stated in their classic law review article: "The right of privacy does not prohibit any publication of matter which is of public or general interest." *The Right to Privacy*, 4 HARV. L. REV. 193, 214 (1890).

We think it clear that parallel reasoning requires the conclusion that a stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern. The months of negotiations over the proper level of compensation for teachers at the Wyoming Valley West High School were unquestionably a matter of public concern, and respondents were clearly engaged in debate about that concern.

Justice BREYER, with whom Justice O'CONNOR joins, concurring.

I join the Court's opinion. I agree with its narrow holding limited to the special circumstances present here: (1) the radio broadcasters acted lawfully (up to the time of final public disclosure); and (2) the information publicized involved a matter of unusual public concern, namely, a threat of potential physical harm to others. I write separately to explain

why, in my view, the Court's holding does not imply a significantly broader constitutional immunity for the media.

As the Court recognizes, the question before us—a question of immunity from statutorily imposed civil liability—implicates competing constitutional concerns. The statutes directly interfere with free expression in that they prevent the media from publishing information. At the same time, they help to protect personal privacy—an interest here that includes not only the "right to be let alone," *Olmstead v. United States,* 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), but also "the interest ... in fostering private speech[.]" Given these competing interests "on both sides of the equation, the key question becomes one of proper fit." *Turner Broadcasting System, Inc. v. FCC*, 520 U.S. 180, 227 (1997) (BREYER, J., concurring in part).

I would ask whether the statutes strike a reasonable balance between their speech-restricting and speech-enhancing consequences. Or do they instead impose restrictions on speech that are disproportionate when measured against their corresponding privacy and speech-related benefits, taking into account the kind, the importance, and the extent of these benefits, as well as the need for the restrictions in order to secure those benefits? What this Court has called "strict scrutiny"—with its strong presumption against constitutionality—is normally out of place where, as here, important competing constitutional interests are implicated.

The statutory restrictions before us directly enhance private speech. The statutes ensure the privacy of telephone conversations much as a trespass statute ensures privacy within the home. That assurance of privacy helps to overcome our natural reluctance to discuss private matters when we fear that our private conversations may become public. And the statutory restrictions consequently encourage conversations that otherwise might not take place.

At the same time, these statutes restrict public speech directly, deliberately, and of necessity. They include media publication within their scope not simply as a means, say, to deter interception, but also as an end. Media dissemination of an intimate conversation to an entire community will often cause the speakers serious harm over and above the harm caused by an initial disclosure to the person who intercepted the phone call. And the threat of that widespread dissemination can create a far more powerful disincentive to speak privately than the comparatively minor threat of disclosure to an interceptor and perhaps to a handful of others. Insofar as these statutes protect private communications against that widespread dissemination, they resemble laws that would award damages caused through publication of information obtained by theft from a private bedroom.

As a general matter, despite the statutes' direct restrictions on speech, the Federal Constitution must tolerate laws of this kind because of the importance of these privacy and speech-related objectives. Rather than broadly forbid this kind of legislative enactment, the Constitution demands legislative efforts to tailor the laws in order reasonably to reconcile media freedom with personal, speech-related privacy.

Nonetheless, looked at more specifically, the statutes, as applied in these circumstances, do not reasonably reconcile the competing constitutional objectives. Rather, they disproportionately interfere with media freedom. For one thing, the broadcasters here engaged in no unlawful activity other than the ultimate publication of the information another had previously obtained. They "neither encouraged nor participated directly or indirectly in the interception." No one claims that they ordered, counseled, encouraged, or otherwise aided or abetted the interception, the later delivery of the tape by the interceptor to an intermediary, or the tape's still later delivery by the intermediary to the media.

For another thing, the speakers had little or no *legitimate* interest in maintaining the privacy of the particular conversation. That conversation involved a suggestion about "blow[ing] off ... front porches" and "do[ing] some work on some of those guys," thereby raising a significant concern for the safety of others. Where publication of private information constitutes a wrongful

act, the law recognizes a privilege allowing the reporting of threats to public safety. Even where the danger may have passed by the time of publication, that fact cannot legitimize the speaker's earlier privacy expectation. Nor should editors, who must make a publication decision quickly, have to determine present or continued danger before publishing this kind of threat.

Further, the speakers themselves, the president of a teacher's union and the union's chief negotiator, were "limited public figures," for they voluntarily engaged in a public controversy. They thereby subjected themselves to somewhat greater public scrutiny and had a lesser interest in privacy than an individual engaged in purely private affairs.

I emphasize the particular circumstances before us because, in my view, the Constitution permits legislatures to respond flexibly to the challenges future technology may pose to the individual's interest in basic personal privacy. Clandestine and pervasive invasions of privacy, unlike the simple theft of documents from a bedroom, are genuine possibilities as a result of continuously advancing technologies. Eavesdropping on ordinary cellular phone conversations in the street (which many callers seem to tolerate) is a very different matter from eavesdropping on encrypted cellular phone conversations or those carried on in the bedroom. But the technologies that allow the former may come to permit the latter. And statutes that may seem less important in the former context may turn out to have greater importance in the latter. Legislatures also may decide to revisit statutes such as those before us, creating better tailored provisions designed to encourage, for example, more effective privacy-protecting technologies.

Chief Justice REHNQUIST, with whom Justice SCALIA and Justice THOMAS join, dissenting.

Technology now permits millions of important and confidential conversations to occur through a vast system of electronic networks. These advances, however, raise significant privacy concerns. We are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless and cellular telephone conversations. In an attempt to prevent some of the most egregious violations of privacy, the United States, the District of Columbia, and 40 States have enacted laws prohibiting the intentional interception and knowing disclosure of electronic communications. The Court holds that all of these statutes violate the First Amendment insofar as the illegally intercepted conversation touches upon a matter of "public concern," an amorphous concept that the Court does not even attempt to define. But the Court's decision diminishes, rather than enhances, the purposes of the First Amendment, thereby chilling the speech of the millions of Americans who rely upon electronic technology to communicate each day.

To effectuate these important privacy and speech interests, Congress and the vast majority of States have proscribed the intentional interception and knowing disclosure of the contents of electronic communications. See, *e.g.,* 18 U.S.C. § 2511(1)(c) (placing restrictions upon "any person who ... intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication").

The Court correctly observes that these are "content-neutral law[s] of general applicability" which serve recognized interests of the "highest order": "the interest in individual privacy and ... in fostering private speech." It nonetheless subjects these laws to the strict scrutiny normally reserved for governmental attempts to censor different viewpoints or ideas.

There is scant support, either in precedent or in reason, for the Court's tacit application of strict scrutiny.

A content-neutral regulation will be sustained if

> " 'it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.' " *Turner Broadcasting System.*

Here, Congress and the Pennsylvania Legislature have acted " 'without reference to the content of the regulated speech.' " There is no intimation that these laws seek "to suppress unpopular ideas or information or manipulate the public debate" or that they "distinguish favored speech from disfavored speech on the basis of the ideas or views expressed." The antidisclosure provision is based solely upon the manner in which the conversation was acquired, not the subject matter of the conversation or the viewpoints of the speakers. The same information, if obtained lawfully, could be published with impunity. As the concerns motivating strict scrutiny are absent, these content-neutral restrictions upon speech need pass only intermediate scrutiny.

The Court's attempt to avoid these precedents by reliance upon the *Daily Mail* string of newspaper cases is unpersuasive. In these cases, we held that statutes prohibiting the media from publishing certain truthful information—the name of a rape victim, the confidential proceedings before a state judicial review commission, and the name of a juvenile defendant—violated the First Amendment. In so doing, we stated that "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order." *Daily Mail.* Neither this *Daily Mail* principle nor any other aspect of these cases, however, justifies the Court's imposition of strict scrutiny here.

Each of the laws at issue in the *Daily Mail* cases regulated the content or subject matter of speech. This fact alone was enough to trigger strict scrutiny . . . and suffices to distinguish these antidisclosure provisions. But, as our synthesis of these cases in *Florida Star* made clear, three other unique factors also informed the scope of the *Daily Mail* principle.

First, the information published by the newspapers had been lawfully obtained from the government itself. Second, the information in each case was already "publicly available," and punishing further dissemination would not have advanced the purported government interests of confidentiality. Such is not the case here. These statutes only prohibit "disclos[ure]," 18 U.S.C. § 2511(1)(c); 18 Pa. Cons. Stat. § 5703(2) (2000), and one cannot "disclose" what is already in the public domain. Third, these cases were concerned with "the 'timidity and self-censorship' which may result from allowing the media to be punished for publishing certain truthful information." But fear of "timidity and self-censorship" is a basis for upholding, not striking down, these antidisclosure provisions: They allow private conversations to transpire without inhibition. And unlike the statute at issue in *Florida Star,* which had no scienter requirement, these statutes only address those who *knowingly* disclose an illegally intercepted conversation.

These laws are content neutral; they only regulate information that was illegally obtained; they do not restrict republication of what is already in the public domain; they impose no special burdens upon the media; they have a scienter requirement to provide fair warning; and they promote the privacy and free speech of those using cellular telephones. It is hard to imagine a more narrowly tailored prohibition of the disclosure of illegally intercepted communications, and it distorts our precedents to review these statutes under the often fatal standard of strict scrutiny. These laws therefore should be upheld if they further a substantial governmental interest unrelated to the suppression of free speech, and they do.

Congress and the overwhelming majority of States reasonably have concluded that sanctioning the knowing disclosure of illegally intercepted communications will deter the initial interception itself, a crime which is extremely difficult to detect. It is estimated that over 20

million scanners capable of intercepting cellular transmissions currently are in operation . . . . As Congress recognized, "[a]ll too often the invasion of privacy itself will go unknown. Only by striking at all aspects of the problem can privacy be adequately protected."

Nonetheless, the Court faults Congress for providing "no empirical evidence to support the assumption that the prohibition against disclosures reduces the number of illegal interceptions," and insists that "there is no basis for assuming that imposing sanctions upon respondents will deter the unidentified scanner from continuing to engage in surreptitious interceptions." It is the Court's reasoning, not the judgment of Congress and numerous States regarding the necessity of these laws, which disappoints.

The "dry-up-the-market" theory, which posits that it is possible to deter an illegal act that is difficult to police by preventing the wrongdoer from enjoying the fruits of the crime, is neither novel nor implausible. It is a time-tested theory that undergirds numerous laws, such as the prohibition of the knowing possession of stolen goods. We ourselves adopted the exclusionary rule based upon similar reasoning, believing that it would "deter unreasonable searches," by removing an officer's "incentive to disregard [the Fourth Amendment][.]"

The same logic applies here and demonstrates that the incidental restriction on alleged First Amendment freedoms is no greater than essential to further the interest of protecting the privacy of individual communications. Were there no prohibition on disclosure, an unlawful eavesdropper who wanted to disclose the conversation could anonymously launder the interception through a third party and thereby avoid detection. Indeed, demand for illegally obtained private information would only increase if it could be disclosed without repercussion. The law against interceptions, which the Court agrees is valid, would be utterly ineffectual without these antidisclosure provisions.

These statutes undeniably protect this venerable right of privacy. Concomitantly, they further the First Amendment rights of the parties to the conversation. "At the heart of the First Amendment lies the principle that each person should decide for himself or herself the ideas and beliefs deserving of expression, consideration, and adherence." *Turner Broadcasting*. By "protecting the privacy of individual thought and expression," [citation omitted], these statutes further the "uninhibited, robust, and wide-open" speech of the private parties, *New York Times Co. v. Sullivan,* (1964). Unlike the laws at issue in the *Daily Mail* cases, which served only to protect the identities and actions of a select group of individuals, these laws protect millions of people who communicate electronically on a daily basis.

Notes

1. To reach a majority, we need to count Breyer and O'Connor's votes from the concurrence, making it controlling because it is the narrower holding. In the concurrence, Breyer focuses on the exceptionally newsworthy character of the speech, as well as the clean hands of those publicizing the tape. Do you think Breyer is right to view the tape as containing threats of violence? Does it matter whether he is right?
2. *Bartnicki's* majority and concurrence both focus on the balancing of speech interests: allowing this person to speak and invade another person's privacy will have the effect of limiting the speech of that other person. This sometimes leads to tension between two visions of speech-promotion: a vision in which the government does nothing and prohibits no speech and a vision in which the government restricts some speech in the belief that doing so can promote more speech.

Boehner v. McDermott, 484 F.3d 573 (D.C. Cir. 2007)

RANDOLPH, Circuit Judge.

Both parties to this case are members of the United States House of Representatives The complaint alleged that Representative McDermott violated 18 U.S.C. § 2511(1)(c) when he

disclosed a tape recording of an illegally intercepted conversation in which Representative Boehner participated.

In our initial decision in this case, we held that Representative McDermott did not have a First Amendment right to disclose the tape. The Supreme Court vacated our decision and returned the case to us for further consideration in light of *Bartnicki v. Vopper* (2001). We remanded the case to the district court. After the parties engaged in discovery, the district court granted summary judgment in favor of Representative Boehner, awarding him $10,000 in statutory damages, $50,000 in punitive damages, and reasonable attorney's fees and costs. A panel of this court, with one judge dissenting, affirmed . . . . We vacated that decision and ordered the case reheard en banc.

On December 21, 1996, Representative Boehner participated in a conference call with members of the Republican Party leadership, including then-Speaker of the House Newt Gingrich. At the time of the conversation Gingrich was the subject of an investigation by the House Committee on Standards of Official Conduct, commonly known as the House Ethics Committee. Representative Boehner was chairman of the House Republican Conference. The participants discussed how they might deal with an expected Ethics Committee announcement of Gingrich's agreement to accept a reprimand and to pay a fine in exchange for the Committee's promise not to hold a hearing.

Representative Boehner was in Florida when he joined the conference call. He spoke from a cellular telephone in his car. John and Alice Martin, who lived in Florida, used a police radio scanner to eavesdrop on the conversation, in violation of 18 U.S.C. § 2511(1)(a). They recorded the call and delivered the tape in a sealed envelope to the Florida office of then-Representative Karen Thurman. Staff members forwarded the envelope to Thurman's Washington office. On January 8, 1997, Thurman's chief of staff learned that the Martins would be visiting the Washington office. Both Thurman and her chief of staff sought legal advice about accepting the tape, presumably because they knew of its contents and how it had been recorded. At some point they consulted then-Representative David Bonior's chief of staff and legislative director. Stan Brand, former General Counsel to the House of Representatives, advised that the tape should not be accepted under any circumstances and that it should be turned over to the Ethics Committee or other appropriate authorities. When the Martins arrived at Thurman's office, her chief of staff returned the tape in its unopened envelope and suggested they turn it over to the Ethics Committee.

At about 5 p.m. on January 8, 1997, in a small anteroom adjacent to the Ethics Committee hearing room, the Martins delivered the tape to Representative McDermott in a sealed 8–1/2″ by 11″ envelope. At the time, Representative McDermott was the ranking Democrat on the Ethics Committee. With the envelope the Martins also delivered a business card and a typed letter dated January 8, 1997, and addressed to "Committee On Standards of Official Conduct ... Jim McDermott, Ranking Member." The letter read:

> Enclosed in the envelope you will find a tape of a conversation heard December 21, 1996 at about 9:45 a.m. The call was a conference call heard over a scanner. We felt the information included were [sic] of importance to the committee. We live in the 5th. Congressional District and attempted to give the tape to Congresswoman Karen Thurman. We were advised by her to turn the tape directly over to you. We also understand that we will be granted immunity.
>
> My husband and I work for Columbia County Schools in Columbia County Florida. We pray that committee will consider our sincerity in placing it in your hands.
>
> We will return to our home today.
>
> Thank you for your consideration.

John and Alice Martin

After conversing with the Martins, Representative McDermott accepted the envelope and returned to the Ethics Committee hearing room.

Later that evening, during a recess, Representative McDermott left the Ethics Committee hearing room and went to his office. There he opened the Martins' envelope, emptied the contents, and listened to the tape. Still later, he called two reporters: Jeanne Cummings of *The Atlanta Journal–Constitution,* for whom he left a message, and Adam Clymer of *The New York Times,* whom he reached. Clymer went to Representative McDermott's office, listened to the tape, and made a recording of it. Cummings returned Representative McDermott's call the next day and came to his office and listened to the tape.

The contents of the tape had substantial news value. In particular, the tape revealed information bearing on whether Gingrich had violated his settlement agreement with the Ethics Committee. On January 10, 1997, *The New York Times* published a front-page article by Clymer entitled "Gingrich Is Heard Urging Tactics in Ethics Case."

On January 13, 1997, the Martins held a press conference and identified Representative McDermott as the congressman to whom they had delivered the tape. Representative McDermott then sent copies of the tape to the offices of the Ethics Committee and resigned from the Committee. The Committee Chairman, then-Representative Nancy Johnson, forwarded the tape to the Department of Justice. The government prosecuted the Martins for violating 18 U.S.C. § 2511(1)(a), which forbids unauthorized interception of "wire, oral, or electronic communication." The Martins pled guilty and were fined $500.

On cross motions for summary judgment, the district court held that Representative McDermott violated 18 U.S.C. § 2511(1)(c) when he disclosed the tape to the reporters. Section 2511(1)(c) makes intentional disclosure of any illegally intercepted conversation a criminal offense if the person disclosing the communication knew or had "reason to know" that it was so acquired. The district court viewed the crucial issue to be whether Representative McDermott lawfully obtained the tape from the Martins. The court held there was no genuine issue of material fact that the Martins' letter to Representative McDermott had been outside of the envelope containing the tape and that Representative McDermott must have read it. This established that Representative McDermott, when he accepted the tape, knew the Martins had illegally intercepted the conversation and illegally disclosed it to him. It followed that he did not lawfully obtain the tape. On appeal, a divided panel of this court agreed that Representative McDermott obtained the tape unlawfully, but for reasons other than those the district court gave.

This is an as-applied challenge to 18 U.S.C. § 2511(1)(c). The question therefore is whether Representative McDermott had a First Amendment right to disclose to the media this particular tape at this particular time given the circumstances of his receipt of the tape, the ongoing proceedings before the Ethics Committee, and his position as a member of the Committee. In answering this question we shall assume arguendo that Representative McDermott lawfully obtained the tape from the Martins.

Whatever the *Bartnicki* majority meant by "lawfully obtain," (Breyer, J., joined by O'Connor, J., concurring), the decision does not stand for the proposition that anyone who has lawfully obtained truthful information of public importance has a First Amendment right to disclose that information. *Bartnicki* avoided laying down such a broad rule of law, and for good reason. There are many federal provisions that forbid individuals from disclosing information they have lawfully obtained. The validity of these provisions has long been assumed. Grand jurors, court reporters, and prosecutors, for instance, may "not disclose a matter occurring before the grand jury." Fed. R. Crim. P. 6(e)(2)(B). The Privacy Act imposes criminal penalties on government employees who disclose agency records containing information about identifiable individuals to unauthorized persons. The Espionage Act punishes officials who

willfully disclose sensitive national defense information to persons not entitled to receive it. The Intelligence Identities Protection Act prohibits the disclosure of a covert intelligence agent's identity. Employees of the Internal Revenue Service, among others, may not disclose tax return information. State motor vehicle department employees may not make public information about an individual's driver's license or registration. Employees of the Social Security Administration, as well as other government employees, may not reveal social security numbers or records . . .[2] Judicial employees may not reveal confidential information received in the course of their official duties. And so forth.

In analogous contexts the Supreme Court has sustained restrictions on disclosure of information even though the information was lawfully obtained. The First Amendment did not shield a television station from liability under the common law right of publicity when it filmed a plaintiff's "human cannonball" act and broadcast the film without his permission. When a newspaper divulged the identity of an individual who provided information to it under a promise of confidentiality, the First Amendment did not provide the paper with a defense to a breach of contract claim. *Cohen v. Cowles Media Co.*, 501 U.S. 663, 670 (1991). The First Amendment did not prevent the government from enforcing reasonable confidentiality restrictions on former employees of the CIA. *See Snepp v. United States*, 444 U.S. 507, 509–10 (1980). Parties to civil litigation did not "have a First Amendment right to disseminate, in advance of trial, information gained through the pretrial discovery process." *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 22, 37 (1984).

In *United States v. Aguilar,* 515 U.S. 593 (1995), a case closely analogous to this one, the Supreme Court held that the First Amendment did not give a federal judge, who obtained information about an investigative wiretap from another judge, the right to disclose that information to the subject of the wiretap. The judge challenged his conviction for violating 18 U.S.C. § 2232(c), which prohibits the improper disclosure of an investigative wiretap. In rejecting his First Amendment claim, the Court wrote that the judge was not "simply a member of the general public who happened to lawfully acquire possession of information about the wiretap; he was a Federal District Court Judge who learned of a confidential wiretap application from the judge who had authorized the interception, and who wished to preserve the integrity of the court. Government officials in sensitive confidential positions may have special duties of non-disclosure."

Aguilar stands for the principle that those who accept positions of trust involving a duty not to disclose information they lawfully acquire while performing their responsibilities have no First Amendment right to disclose that information. The question thus becomes whether, in the words of *Aguilar,* Representative McDermott's position on the Ethics Committee imposed a "special" duty on him not to disclose this tape in these circumstances. *Bartnicki* has little to say about that issue. The individuals who disclosed the tape in that case were private citizens who did not occupy positions of trust.

All members of the Ethics Committee, including Representative McDermott, were subject to Committee Rule 9, which stated that "Committee members and staff shall not disclose any evidence relating to an investigation to any person or organization outside the Committee unless authorized by the Committee." This rule recognizes the unique role of the Ethics Committee and reflects a desire "to protect the rights of individuals accused of misconduct, preserve the integrity of the investigative process, and cultivate collegiality among Committee members[.]"

---

[2] The government can also limit disclosures by persons who are not its employees without running afoul of the First Amendment. Private attorneys who reveal their clients' confidences may be punished for doing so. And those who sell or rent video tapes or DVDs ordinarily may not reveal "personally identifiable information concerning" their customers. *See* 18 U.S.C. § 2710(b).

The House has the power to make and enforce such rules under the Rulemaking Clause of the Constitution, which states that "Each House may determine the Rules of its Proceedings, punish its Members for disorderly Behaviour, and, with the Concurrence of two thirds, expel a Member," U.S. Const. art. I, § 5, cl. 2. There is no question that the rules themselves are reasonable and raise no First Amendment concerns. Counsel for Representative McDermott conceded that the House could, consistent with the First Amendment, punish Representative McDermott if it determined he had violated its rules by releasing the Martins' tape to the media.

If the First Amendment does not protect Representative McDermott from House disciplinary proceedings, it is hard to see why it should protect him from liability in this civil suit. Either he had a First Amendment right to disclose the tape to the media or he did not. If he had the right, neither the House nor the courts could impose sanctions on him for exercising it. If he did not have the right, he has no shield from civil liability or from discipline imposed by the House. In that event, his civil liability would rest not on his breach of some ethical duty, but on his violation of a federal statute for which he had no First Amendment defense. The situation is the same as that in *Aguilar*. There the defendant-judge was punished not for violating his ethical duty to maintain judicial secrecy, but for violating the general prohibition on disclosing investigative searches.

The only remaining question is whether the tape fell within Representative McDermott's duty of confidentiality under the rules of the House and the Ethics Committee. Here we can be confident that the rules covered Representative McDermott's handling of the tape.

Notes

1. At the close of *Bartnicki*, students are sometimes left with the impression that few privacy restrictions are permissible under the First Amendment. This is not the case, as *Boehner* makes clear. Many individuals operate under requirements of confidentiality or secrecy. They may "lawfully obtain" information in the sense that they are lawfully given it, but that lawful acquisition is not receiving title to it free and clear. To peek ahead to medical privacy: your doctor has a duty of confidentiality toward you. If they breach that duty by disclosing your highly newsworthy medical information to the press, they can be sued civilly and prosecuted criminally. *Bartnicki* holds that the media may be allowed to publish that information, but does not save the doctor. If the doctor wants to safely disclose confidential information, they need to do so within the carefully limited exceptions permitted under medical privacy law.
2. *Boehner* does draw a dissent (omitted), and readers should not be left with the idea that this area of law is neat. It is not. Grey areas abound. But some points are generally agreed: a) many government actors obtain confidential or secret information as part of their jobs and are not allowed to share it despite the First Amendment; b) many private professionals, particularly doctors and lawyers, operate under government-mandated duties of confidentiality despite the First Amendment; c) private citizens can contract to suppress each other's speech and those contracts are generally enforceable despite the First Amendment.[25] Any good legal ethics class will explain that attorney-client privilege is complicated and subject to exceptions and limitations, but there is no doubt that such a thing as attorney-client privilege exists. First Amendment doctrine is always engaged in rights-balancing.

[25] There are legal limitations on nondisclosure agreements. For instance, a nondisclosure agreement aimed at concealing criminal activity will not be enforceable. The broader question of which NDAs should be unenforceable as a matter of public policy is constantly evolving.

C. False Light and Defamation

1) False light

The third privacy tort is "publicity placing person in false light." According to the Restatement (Second) of Torts (§ 652E),

> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if
>
> A. the false light in which the other was places would be highly offensive to a reasonable person, and
>
> B. the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

The power of a false light claim is that it can rely on false implications and is not restricted to clearly false statements. The weakness is that it requires publicity and not just disclosure to a single additional person. Also, false light is generally considered to be about emotional harm rather than harm to reputation (which is the domain of defamation).

Notes

1. False light claims sometimes arise when irrelevant photos are published alongside injurious material. For instance, plaintiffs were allowed to proceed with their false light claim when their publicly available photos were republished as part of promotional material for a strip club with which they were not affiliated. *Longoria v. Kodiak Concepts LLC*, 527 F.Supp.3d 1085 (D. Ariz. 2021). It appears that the club thought it could use the photos because they were publicly available and not manipulated. Plaintiffs also proceeded on a right of publicity claim (see II.D below for the elements of that tort).
2. In *Khodorkovskaya v. Gay*, 5 F.4th 80 (D.C. Cir. 2021), a plaintiff brought suit against a playwright who wrote a fictional play inspired by real events that depicted her as a prostitute and murderer. The court held that a false light claim could not proceed: "[T]he scene could not reasonably be understood to convey actual facts about the real-life Inna. The scene takes place directly in the wake of Putin's character reciting an absurdist poem to the live audience and would be viewed by them in the immediate light of that pronounced example of dramatic license and fictional device."
3. Some states do not recognize false light as a cause of action. For example, Florida rejects false light on the grounds that it was largely duplicative of defamation and lacks the clear First Amendment protections present in defamation law. *Jews for Jesus, Inc. v. Rapp* 997 So. 2d 1098 (Fl. S.C. 2008). In reaching this conclusion, the Florida Supreme Court noted that false light is the least recognized of the four privacy torts and that it was rare – in jurisdictions accepting false light – to find a case that was based solely upon a false light claim.

2) Defamation

Defamation substantially predates Prosser's privacy torts. It naturally fits in with the other causes of action, however, as it is similar to false light and is often brought alongside public disclosure of private facts claims. It is not uncommon to bring a public disclosure cause of action over true claims and a defamation cause of action over false ones in the same suit.

Under the Restatement (Second) of Torts § 558, to create liability for defamation there must be:

1. a false and defamatory statement concerning another;
2. an unprivileged publication to a third party;
3. fault amounting at least to negligence on the part of the publisher; and
4. [Harm or per se injury]

Consider the double-barreled first element. "False" requires a statement to be a claim of fact and to not be correct; truth is an absolute defense to defamation. "Defamatory" requires some explanation. A statement is defamatory if it tends to injure the reputation of another or deters third parties from associating or dealing with them. Falsely calling someone a drug addict is defamatory. Calling someone a resident of New Jersey, even if false, will generally not be.[26] Some categories of defamation are presumed to be harmful, meaning that plaintiffs need not show actual damages. These categories are:

1. Saying that someone committed a crime or immoral conduct
2. Saying that someone had a contagious, infectious, or "loathsome" disease
3. Saying someone engaged in sexual misconduct or was unchaste
4. Saying something harmful about someone's business, trade, or profession

Imagine I falsely claim that the mayor had worked as a prostitute when he was younger. It might be that people would generally not mind. It fits three of the four above categories, however, because (1) prostitution is illegal in much of the country and many would call it immoral, (3) it counts as sexual misconduct, and (4) a history of criminal activity is inconsistent with his role as an elected official. So the false statement would likely be defamation per se. One could argue that the statement was not meant literally, however. It would likely be a statement of opinion or hyperbole to say "the mayor is a prostitute; he'll do anything for a campaign contribution."

Eramo v. Rolling Stone, LLC, 209 F.Supp.3d 862 (W.D. Va. 2016)

Glen E. Conrad, Chief United States District Judge

Nicole Eramo [Associate Dean of Students at the University of Virginia ("UVA")] filed this defamation action against defendants Rolling Stone, Sabrina Rubin Erdely, and Wenner Media. The case is presently before the court on plaintiff's motion for partial summary judgment and defendants' motion for summary judgment.

On November 19, 2014, defendants published an article written by Erdely and entitled "A Rape on Campus: A Brutal Assault and Struggle for Justice at UVA." The Article contained a graphic depiction of the alleged gang-rape of a UVA student, referred to as "Jackie," at a Phi Kappa Psi fraternity party. According to the Article, Jackie's mother informed an academic dean that Jackie had a "bad experience" at a party. The academic dean then put Jackie in touch with Eramo.

At the time, Eramo's duties at UVA included performing intake of sexual assault complaints and providing support to purported victims. On campus, Eramo was seen as "an expert in all issues related to sexual assault" and the "point person" for reports of sexual misconduct.

In her pitch to Rolling Stone, Erdely stated that her article would "focus on a sexual assault case on one particularly fraught campus . . . following it as it makes its way through university procedure to its resolution, or lack thereof." The Article describes Jackie's

[26] Were the person running for office in New York City and claiming to be a New York resident, saying that they are lying and are actually a resident of New Jersey might be defamatory, however.

interactions with Eramo, including how Jackie shared information about two other victims of the same fraternity. Throughout her investigation, Erdely spoke with a number of students about sexual assault at UVA; her notes reflect that several students communicated their admiration of Eramo. As publication neared, some students expressed to Erdely concerns that her portrayal of Eramo was inaccurate.

Erdely relied heavily on the narrative Jackie provided in writing the Article, so much so that she did not obtain the full names of Jackie's assailants or contact them. Nor did Erdely interview the individuals who found Jackie the night of her alleged gang-rape. Similarly, Erdely did not obtain certain corroborating documents Jackie claimed to have access to and was unable to confirm with Jackie's mother Jackie's assertion that her mother had likely destroyed the dress Jackie wore on the night of the alleged rape. Additionally, Erdely was not granted an interview with Eramo to ask about the university's policies. Instead, Eramo's superiors made UVA President, Teresa Sullivan, available.

After its release, the Article created a "media firestorm" and was viewed online more than 2.7 million times.

The complaint asserts that the Article and subsequent media appearances destroyed Eramo's reputation as an advocate and supporter of victims of sexual assault. She was attacked by individuals on television and the internet, and she received hundreds of threatening, vicious emails from members of the public. As a result, Eramo suffered "significant embarrassment, humiliation, mental suffering and emotional distress."

Upon further investigation by independent entities, it was reported that the Article, and key components of Jackie's story, could not be substantiated. Within two weeks of the Article's publication, the fraternity where Jackie's alleged attack took place produced evidence demonstrating that no social gathering was held on the night in question and that no member of the fraternity matched the description given by Jackie for her primary attacker. Additionally, *The Washington Post* ran an article addressing the fact that Erdely did not contact Jackie's accused assailants.

On December 5, 2014, Rolling Stone issued a statement (the "Editor's Note") that acknowledged the discrepancies in Jackie's account, blamed Jackie for misleading Erdely, and claimed that its trust in Jackie had been "misplaced." In April 2015, after a report by the *Columbia Journalism Review* described the Article as a "journalistic failure" and concluded that defendants "set aside or rationalized as unnecessary essential practices of reporting," Rolling Stone "officially retracted" and removed the Article from its website.

On May 12, 2015, Eramo filed a six-count defamation action arising not only from the allegations in the Article but also from other statements made by the defendants in subsequent media appearances.

I. Public Official or Limited-Purpose Public Figure

Both sides have moved for summary judgment on the issue of whether Eramo was a public official or a limited-purpose public figure. If Eramo was a public official or limited-purpose public figure at the time of publication, as part of her defamation case, she must prove by clear and convincing evidence that defendants acted with actual malice. *New York Times Co. v. Sullivan* (1964); *Gertz v. Robert Welch* (1974). The issue of whether Eramo was a public official or limited-purpose public figure is a question of law to be resolved by the court.

A limited-purpose public figure is one who "voluntarily injects himself or is drawn into a particular public controversy and thereby becomes a public figure for a limited range of issues." Importantly, these individuals are subject to the actual malice standard for two reasons: (1) because of "their ability to resort to the 'self-help' remedy of rebuttal" as these individuals "usually enjoy significantly greater access [to the media] than private individuals"; and (2) because they have "voluntarily exposed themselves to increased risk of injury from

defamatory falsehood." To determine whether a plaintiff is a private person or a limited-purpose public figure in relation to a particular public controversy, defendants must prove the following:

> "(1) the plaintiff had access to channels of effective communication; (2) the plaintiff voluntarily assumed a role of special prominence in the public controversy; (3) the plaintiff sought to influence the resolution or outcome of the controversy; (4) the controversy existed prior to the publication of the defamatory statement; and (5) the plaintiff retained public-figure status at the time of the alleged defamation."

The second and third factors are often combined and are the heart of the inquiry: "whether the plaintiff had voluntarily assumed a role of special prominence in a public controversy by attempting to influence the outcome."

Here, a fair reading of the Article suggests that the controversy at issue is UVA's response to allegations of sexual assault. The record warrants the determination that Eramo voluntarily assumed a position of "special prominence" on this issue: she took advantage of her access to local media, specifically by appearing on WUVA, providing input to *The Cavalier Daily*, and speaking to local affiliates of national news networks. Furthermore, the volume of her media appearances, and in some instances their depth, supports the conclusion that Eramo attempted to influence the outcome of the controversy. In 2013, for instance, Eramo authored an opinion piece regarding the University's process for handling sexual assault complaints. The court thus concludes that defendants have met their burden as to the second and third factors.

Regarding the fourth and fifth factors, Eramo's numerous local media appearances and their temporal proximity to the Article, in addition to the Office of Civil Rights investigation UVA was under at the time, indicate that the controversy at issue, UVA's response to allegations of sexual assault, existed prior to publication of the Article.

II. Actual Malice

A public official, public figure, or limited-purpose public figure may recover for a defamatory falsehood only on a showing of "actual malice." *New York Times Co. v. Sullivan*; *Gertz v. Robert Welch*. Actual malice "requires at a minimum that the statements were made with reckless disregard for the truth." Reckless disregard means that defendants must have "entertained serious doubts as to the truth of [their] publication." Furthermore, because actual malice is a subjective inquiry, a plaintiff "is entitled to prove the defendant's state of mind through circumstantial evidence."

It is helpful to review what other courts have determined is and is not sufficient evidence. For example, it is well settled that "failure to investigate will not alone support a finding of actual malice." *Harte-Hanks Commc'ns., Inc. v. Connaughton* (1989); *see also Biro v. Conde Nast* (2d Cir. 2015) ("We recognize that although failure to investigate does not in itself establish bad faith, reliance on anonymous or unreliable sources without further investigation may support an inference of actual malice."). Similarly, departure from journalistic standards is not a determinant of actual malice, but such action might serve as supportive evidence. "Repetition of another's words does not release one of responsibility if the repeater knows that the words are false or inherently improbable, or there are obvious reasons to doubt the veracity of the person quoted." *Goldwater v. Ginzburg* (2d Cir. 1969). Furthermore, while actual malice cannot be inferred from ill will or intent to injure alone, "[i]t cannot be said that evidence of motive or care never bears any relation to the actual malice inquiry." *Connaughton*.

Here, as in most similar cases, plaintiff largely relies on circumstantial evidence. Although failure to adequately investigate, a departure from journalistic standards, or ill will or intent to injure will not singularly provide evidence of actual malice, the court believes that proof of all three is sufficient to create a genuine issue of material fact. Plaintiff, however, goes further. Pointing to Erdely's own reporting notes, plaintiff also forecasts evidence that could

lead a reasonable jury to find that Erdely had "obvious reasons to doubt [Jackie's] veracity" or "entertained serious doubts as to the truth of [her] publication."

First, plaintiff offers evidence that could lead a jury to determine that Erdely had a preconceived story line and may have consciously disregarded contradictory evidence. A jury could conclude from Erdely's pitch for the Article that Erdely expected to find inaction from the university's administration. She described how the Article would highlight "the various ways colleges have resisted involvement on the issue of sexual assault on campus; [and how it would] focus on a sexual assault case on campus . . . following it as it makes its way through university procedure to its resolution, or lack thereof." "Erdely had also previously published five similar articles, and deposition testimony suggests that students felt that Erdely did not listen to what they told her about Eramo.

Second, plaintiff has produced evidence supporting the inference that Erdely should have further investigated Jackie's allegations. The record suggests that Erdely knew the identity of at least one of the individuals who found Jackie the night of her alleged rape. Erdely, however, did not seek to contact this individual. Plaintiff cites evidence that could lead a factfinder to determine that others at Rolling Stone knew Erdely did not reach out to these individuals to corroborate Jackie's story. Erdely's notes similarly reveal that Jackie had told Elderly she possessed, or at least had access to, certain documents that could have corroborated her story of the rape. Erdely never received a copy of these documents, and Erdely's notes imply inconsistencies in Jackie's claims about them. From these facts, a reasonable jury could conclude that Erdely should have investigated further, and that her failure to do so could imply that Erdely acted with actual malice.

Third, plaintiff has presented evidence suggesting that Erdely had reasons to doubt Jackie's credibility. Erdely noted disbelief about Jackie's assertion as to the identities of the two other victims; Erdely was put on notice that Jackie's alleged rape, by individuals supposedly being recruited into the fraternity, occurred several months before fraternity recruitment events; and that Erdely found Jackie's story of three women being gang-raped at the same fraternity "too much of a coincidence." Erdely was aware that Jackie's account of her alleged rape had changed but, nonetheless, did not press Jackie to explain the inconsistencies. Moreover, a jury could find that Rolling Stone knew that Jackie's version of the story had not been vetted. Deposition of Elisabeth Garber-Paul [Rolling Stone fact checker] (stating she knew that Rolling Stone had not reached out to certain individuals who were quoted in the Article and alleged to have found Jackie on the night of the rape, in part, because Jackie refused to provide their contact information).

Fourth, plaintiff offers evidence suggesting that at least three individuals advised Erdely that her portrayal of Eramo was inaccurate.

Arguably, a reasonable jury could find that none of the evidence presented independently supports a finding of actual malice by clear and convincing evidence. Taken as a whole, however, a jury could conclude otherwise. Therefore, the court heeds the Fourth Circuit's admonition that summary judgment should be employed carefully when addressing a party's subjective state of mind.

III. The Challenged Statements

Both sides have also moved for summary judgment on the issue of whether the challenged statements are actionable. "In Virginia, the elements of libel are (1) publication of (2) an actionable statement with (3) the requisite intent." To be actionable, a statement must contain a "provably false factual connotation," must be "of or concerning" the plaintiff, and must "tend[ ] to harm the reputation [of the plaintiff]." It is for the court to decide whether a statement has a provably false factual connotation or is protected opinion and whether a statement is capable of having a defamatory meaning, that is, tending to harm the plaintiff's reputation.

In deciding whether statements convey a factual connotation or are protected opinion, the court looks to "the context and tenor of the article," whether the language is "loose, figurative, or hyperbolic language which would negate the impression that the writer" is making a factual assertion, and whether the statement is "subject to objective verification." "Locating the line separating constitutionally protected speech from actionable defamation can be difficult and requires consideration of the nature of the language used and the context and general tenor of the article to determine whether the statement can reasonably be viewed as an assertion of actual fact." If "a reasonable factfinder could conclude that the statements . . . imply an assertion [of fact]," the statements are not protected.

Merely because the statements may be deemed to have a false factual connotation, however, is not sufficient to support a defamation action. The statements must also be capable of having a defamatory meaning. A statement that "tends to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him" has a defamatory meaning. In determining whether a statement is capable of having a defamatory meaning, the court considers the plain and natural meaning of the words in addition to the inferences fairly attributable to them. However, whether the plaintiff was actually defamed remains a question to be resolved by the factfinder.

Defendants argue that the challenged statements are not actionable because, as a matter of law, they are protected opinion and not capable of harming Eramo's reputation. In contrast, plaintiff contends that the challenged statements are factual and defamatory *per se*. "[A] statement is defamatory *per se* if it, among other circumstances, . . . 'impute[s] to a person unfitness to perform the duties of an office or employment of profit, or want of integrity in the discharge of the duties of such an office or employment.'"

After reviewing the Article, the court believes that it is not "clear to all reasonable listeners" that all twelve statements targeted by the plaintiff are "exaggerated rhetoric" or "the opinion of the author." Contrary to the talk-show host in *CACI Premier Tech., Inc. v. Rhodes* (4th Cir. 2008), Erdely has not admitted to "making frequent use of hyperbole." On the contrary, Erdely has written at least five other similarly styled, solemn and fact-intensive articles about rape. These circumstances support the notion that "A Rape on Campus" was largely a report of a factual occurrence. Likewise, the characterization of the article as an investigation in subsequent interviews bolsters the court's understanding that the general tenor of the Article, and reasonable understanding of it, is one of factual assertion.

As to the remaining statements, the court is persuaded that a reasonable understanding is that they assert factual connotations regarding Eramo and the administration's actions. For example, a jury could find that the "trusted UVA dean" either did or did not discourage Jackie from sharing her story, that Eramo did or did not tell Jackie that "nobody wants to send their daughter to the rape school," and that Eramo did or did not have a nonreaction to Jackie's assertion that two other individuals were raped at the same fraternity. Even the statements asserting that the administration should have acted in light of Jackie's allegation that two other individuals were raped at the Phi Kappa Psi fraternity is capable of conveying a verifiable fact: that the administration did not act. Therefore, the court finds the remaining challenged statements impart what a reasonable reader would believe to be factual. Similarly, considering all reasonable inferences, the court believes that the statements are capable of having a defamatory meaning.

Plaintiff, however, asks the court to further find that the challenged statements are defamatory *per se*. As with actual malice, it is instructive to review what other courts have found to be defamatory *per se*. For example, in *Cretella v. Kuzminkski* (E.D. Va. 2009), the district court found the assertions that plaintiff caused embarrassment to his employer and was in danger of losing his professional license to be defamatory *per se*. Similarly, in *Carwile v. Richmond Newspapers* (Va. 1954), statements implying that the plaintiff was guilty of conduct for which "the plaintiff could and should be subject to disbarment proceedings" were held to be

defamatory *per se*. Here, however, the court believes that the alleged defamatory meaning ascribed to the challenged statements does not give rise to presumed damages. This is not to imply that Eramo has or has not been damaged; it is to keep the determination of damages, and the determination of whether the statements actually defamed Eramo, with the factfinder.

Notes

1. It is hard for a public figure to win a defamation claim, yet it happens. And we have seen a wave of defamation lawsuits in recent years. In addition to this case against Rolling Stone, there have been big verdicts and settlements against Fox News for its handling of Dominion Voting Systems after the 2020 election, Donald Trump for various denials of sexual assault claims, Alex Jones for promoting conspiracy theories about the Sandy Hook shootings, and Rudy Giuliani for promoting conspiracy theories about particular election workers. Defaming people can be expensive.
2. *Fact versus opinion*. "Professor A is racist" is an opinion. "Professor A is racist. He regularly belittles racial minorities in class" is a claim of fact. Whether the professor regularly belittles minorities in class is a statement that can be true or false, and that statement is plainly linked to the prior opinion and serves as support for it. "The President is a senile old man" is an opinion. "The President is so old that he cannot tie his own shoes" is *probably* hyperbole and not a statement of fact. Under certain circumstances, however, that statement could be taken as a fact claim.
3. As the judge here observes, a public figure (or public official) needs to prove actual malice to win a defamation claim. This is in part to foster a vigorous debate about public figures and issues and in part because, as the court focuses on here, public figures can defend themselves in the popular press. A private figure claiming defamation on a matter of purely private concern, for example a company suing over a false Google review, may need to only show negligence in order to win.
4. Actual malice is most easily shown with knowing falsehoods. Imagine Person A is in a romantic relationship with Person B. After the relationship ends, Person A claims that Person B was repeatedly physically abusive. Person A presumably knows whether that statement is true. The required *mens rea* is therefore largely irrelevant; the only major question in the case is whether the statement is true.
5. *Why defamation is a privacy topic*. Privacy is about many things, but among them is the ability to control how one is presented to other people. Public disclosure is about controlling true statements about the self. Defamation is about controlling false statements about the self. The right of publicity is about controlling commercial statements about the self.

3) Section 230 as a bar to liability

Section 230 of the Communications Decency Act provides,

> (c) PROTECTION FOR "GOOD SAMARITAN" BLOCKING AND SCREENING OF OFFENSIVE MATERIAL
>
> > (1) TREATMENT OF PUBLISHER OR SPEAKER. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
> >
> > (2) CIVIL LIABILITY. No provider or user of an interactive computer service shall be held liable on account of—
> >
> > > (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or

> otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in [in paragraph A, above].

The focus of most Section 230 discussion is Section 230(c)(1). This grant of immunity applies only if the interactive computer service provider is not itself an "information content provider" with respect to the content, which is defined as someone who is "responsible, in whole or in part, for the creation or development of" the offending content. Section 230(f)(3).

In short, Section 230 allows websites like X, Facebook, and Yelp to function the way they do even though some people will inevitably post defamatory content on them. The websites themselves are not liable for the bad acts of those who post there. Section 230 is not without exceptions and limitations, however. For instance, Roommates.com could be pursued under the Fair Housing Act because Roommates.com itself directly facilitated the filtering of roommate searches by race, sex, and other protected characteristics. *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC,* 521 F.3d 1157 (9th Cir. 2008). Allowing users to post that they want a "white roommate" does not remove Section 230 immunity. Allowing users to filter results by race does.

Further, there are statutory limitations to the scope of Section 230. Section 230 does not "impair the enforcement" of federal criminal law, any law (state or federal) pertaining to intellectual property, any of several laws about sex trafficking and the facilitation of prostitution, or the Electronic Communications Privacy Act. Section 230(e).

Nevertheless, Section 230 applies to many civil privacy claims and is repeatedly invoked and criticized in the cyber-harassment domain.

Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997)

WILKINSON, Chief Judge:

Kenneth Zeran brought this action against America Online, Inc. ("AOL"), arguing that AOL unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter.

"The Internet is an international network of interconnected computers," currently used by approximately 40 million people worldwide. *Reno v. ACLU* (1997). One of the many means by which individuals access the Internet is through an interactive computer service. These services offer not only a connection to the Internet as a whole, but also allow their subscribers to access information communicated and stored only on each computer service's individual proprietary network. AOL is just such an interactive computer service. Much of the information transmitted over its network originates with the company's millions of subscribers. They may transmit information privately via electronic mail, or they may communicate publicly by posting messages on AOL bulletin boards, where the messages may be read by any AOL subscriber.

The instant case comes before us on a motion for judgment on the pleadings, so we accept the facts alleged in the complaint as true. On April 25, 1995, an unidentified person posted a message on an AOL bulletin board advertising "Naughty Oklahoma T–Shirts." The posting described the sale of shirts featuring offensive and tasteless slogans related to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Those interested in purchasing the shirts were instructed to call "Ken" at Zeran's home phone number in Seattle, Washington. As a result of this anonymously perpetrated prank, Zeran received a high volume of calls, comprised primarily of angry and derogatory messages, but also including death

threats. Zeran could not change his phone number because he relied on its availability to the public in running his business out of his home. Later that day, Zeran called AOL and informed a company representative of his predicament. The employee assured Zeran that the posting would be removed from AOL's bulletin board but explained that as a matter of policy AOL would not post a retraction. The parties dispute the date that AOL removed this original posting from its bulletin board.

On April 26, the next day, an unknown person posted another message advertising additional shirts with new tasteless slogans related to the Oklahoma City bombing. Again, interested buyers were told to call Zeran's phone number, to ask for "Ken," and to "please call back if busy" due to high demand. The angry, threatening phone calls intensified. Over the next four days, an unidentified party continued to post messages on AOL's bulletin board, advertising additional items including bumper stickers and key chains with still more offensive slogans. During this time period, Zeran called AOL repeatedly and was told by company representatives that the individual account from which the messages were posted would soon be closed. Zeran also reported his case to Seattle FBI agents. By April 30, Zeran was receiving an abusive phone call approximately every two minutes.

Meanwhile, an announcer for Oklahoma City radio station KRXO received a copy of the first AOL posting. On May 1, the announcer related the message's contents on the air, attributed them to "Ken" at Zeran's phone number, and urged the listening audience to call the number. After this radio broadcast, Zeran was inundated with death threats and other violent calls from Oklahoma City residents. Over the next few days, Zeran talked to both KRXO and AOL representatives. He also spoke to his local police, who subsequently surveilled his home to protect his safety. By May 14, after an Oklahoma City newspaper published a story exposing the shirt advertisements as a hoax and after KRXO made an on-air apology, the number of calls to Zeran's residence finally subsided to fifteen per day.

Zeran first filed suit on January 4, 1996, against radio station KRXO in the United States District Court for the Western District of Oklahoma. On April 23, 1996, he filed this separate suit against AOL in the same court. Zeran did not bring any action against the party who posted the offensive messages.[1]

Because § 230 was successfully advanced by AOL in the district court as a defense to Zeran's claims, we shall briefly examine its operation here. Zeran seeks to hold AOL liable for defamatory speech initiated by a third party. He argued to the district court that once he notified AOL of the unidentified third party's hoax, AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory material. Section 230 entered this litigation as an affirmative defense pled by AOL. The company claimed that Congress immunized interactive computer service providers from claims based on information posted by a third party.

The relevant portion of § 230 states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1).[2] By its plain language, § 230 creates a

[1] Zeran maintains that AOL made it impossible to identify the original party by failing to maintain adequate records of its users. The issue of AOL's record keeping practices, however, is not presented by this appeal.

[2] Section 230 defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(e)(2). The term "information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." § 230(e)(3). The parties do not dispute that AOL falls within the CDA's "interactive computer

federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred.

The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. In specific statutory findings, Congress recognized the Internet and interactive computer services as offering "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." It also found that the Internet and interactive computer services "have flourished, to the benefit of all Americans, *with a minimum of government regulation.*" Congress further stated that it is "the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, *unfettered by Federal or State regulation.*"

None of this means, of course, that the original culpable party who posts defamatory messages would escape accountability. While Congress acted to keep government regulation of the Internet to a minimum, it also found it to be the policy of the United States "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." Congress made a policy choice, however, not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages.

Congress' purpose in providing the § 230 immunity was thus evident. Interactive computer services have millions of users. The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.

Another important purpose of § 230 was to encourage service providers to self-regulate the dissemination of offensive material over their services. In this respect, § 230 responded to a New York state court decision, *Stratton Oakmont, Inc. v. Prodigy Servs. Co.* (N.Y. Sup. Ct. 1995). There, the plaintiffs sued Prodigy—an interactive computer service like AOL—for defamatory comments made by an unidentified party on one of Prodigy's bulletin boards. The court held Prodigy to the strict liability standard normally applied to original publishers of defamatory statements, rejecting Prodigy's claims that it should be held only to the lower "knowledge" standard usually reserved for distributors. The court reasoned that Prodigy acted more like an original publisher than a distributor both because it advertised its practice of controlling content on its service and because it actively screened and edited messages posted on its bulletin boards.

---

service" definition and that the unidentified third party who posted the offensive messages here fits the definition of an "information content provider."

Congress enacted § 230 to remove the disincentives to self-regulation created by the *Stratton Oakmont* decision. Under that court's holding, computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher. Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted § 230's broad immunity "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. § 230(b)(4). In line with this purpose, § 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions.

Zeran argues, however, that the § 230 immunity eliminates only publisher liability, leaving distributor liability intact. Publishers can be held liable for defamatory statements contained in their works even absent proof that they had specific knowledge of the statement's inclusion. According to Zeran, interactive computer service providers like AOL are normally considered instead to be distributors, like traditional news vendors or book sellers. Distributors cannot be held liable for defamatory statements contained in the materials they distribute unless it is proven at a minimum that they have actual knowledge of the defamatory statements upon which liability is predicated. Zeran contends that he provided AOL with sufficient notice of the defamatory statements appearing on the company's bulletin board. This notice is significant, says Zeran, because AOL could be held liable as a distributor only if it acquired knowledge of the defamatory statements' existence.

Because of the difference between these two forms of liability, Zeran contends that the term "distributor" carries a legally distinct meaning from the term "publisher." Accordingly, he asserts that Congress' use of only the term "publisher" in § 230 indicates a purpose to immunize service providers only from publisher liability. He argues that distributors are left unprotected by § 230 and, therefore, his suit should be permitted to proceed against AOL. We disagree. Assuming *arguendo* that Zeran has satisfied the requirements for imposition of distributor liability, this theory of liability is merely a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230.

The terms "publisher" and "distributor" derive their legal significance from the context of defamation law. Although Zeran attempts to artfully plead his claims as ones of negligence, they are indistinguishable from a garden variety defamation action. Because the publication of a statement is a necessary element in a defamation action, only one who publishes can be subject to this form of tort liability. Publication does not only describe the choice by an author to include certain information. In addition, both the negligent communication of a defamatory statement and the failure to remove such a statement when first communicated by another party—each alleged by Zeran here under a negligence label—constitute publication. In fact, every repetition of a defamatory statement is considered a publication.

In this case, AOL is legally considered to be a publisher. "[E]very one who takes part in the publication . . . is charged with publication." Even distributors are considered to be publishers for purposes of defamation law:

> Those who are in the business of making their facilities available to disseminate the writings composed, the speeches made, and the information gathered by others may also be regarded as participating to such an extent in making the books, newspapers, magazines, and information available to others as to be regarded as publishers. They are intentionally making the contents available to others, sometimes without knowing all of the contents—including the defamatory content—and sometimes without any opportunity to ascertain, in advance, that any defamatory matter was to be included in the matter published.

AOL falls squarely within this traditional definition of a publisher and, therefore, is clearly protected by § 230's immunity.

Zeran next contends that interpreting § 230 to impose liability on service providers with knowledge of defamatory content on their services is consistent with the statutory purposes outlined in Part IIA. Zeran fails, however, to understand the practical implications of notice liability in the interactive computer service context. Liability upon notice would defeat the dual purposes advanced by § 230 of the CDA. Like the strict liability imposed by the *Stratton Oakmont* court, liability upon notice reinforces service providers' incentives to restrict speech and abstain from self-regulation.

If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context. Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not.

Similarly, notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services. Any efforts by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and thereby create a stronger basis for liability. Instead of subjecting themselves to further possible lawsuits, service providers would likely eschew any attempts at self-regulation.

More generally, notice-based liability for interactive computer service providers would provide third parties with a no-cost means to create the basis for future lawsuits. Whenever one was displeased with the speech of another party conducted over an interactive computer service, the offended party could simply "notify" the relevant service provider, claiming the information to be legally defamatory.

Notes

1. Section 230 is among the most consequential provisions in cyberlaw. It stands as a barrier to enforcement of many of the laws covered in this section, and proposals to eliminate, amend, and reinterpret it are ubiquitous in the privacy and cybersecurity space. Jeff Kosseff's seminal book on Section 230 is aptly named—*The Twenty-Six Words That Created the Internet*. Things would work differently without it and debates over how much it can be changed and challenged are ongoing.
2. Part of why Section 230 is so frustrating for plaintiffs is that the non-platform defendant, meaning the person who actually posted the content, is often either unidentifiable or broke. It is relatively easy to make oneself difficult to track online for the limited purpose of making a small number of posts or sending a small number of emails. Even if it is technically possible to pierce that anonymity, it may be too hard and too expensive for many plaintiffs. And, of course, this is another battle of privacy interests. Person A's efforts to sue Person B over Person B's anonymous speech are frustrated by Person B's privacy protections.
3. Though Section 230 stops websites from being treated as publishers of third-party content, it does not stop them from being liable for other things. If a website promises to remove particular content and does not then it might be liable under a variety of laws. For instance, it might be sued for breach of contract, promissory estoppel, or a violation of Section 5 of the Federal Trade Commission Act, which prohibits deceptive acts and practices.

D. Right of Publicity

The final privacy tort, the right of publicity, sits at the intersection of privacy and intellectual property. The amorphous cause of action surrounding publicity rights was first dubbed the "right of publicity" in the decidedly economic context of a contract dispute.[27] The court in *Haelan Lab'ys v. Topps Chewing Gum* considered the exploitation of an individual's identity in the context of property law, finding that the right to use photographs could be exclusively granted via contract. The court attributed to such photographs a "pecuniary worth" that ought to be legally enforceable. Such a property interest was construed by the *Motschenbacher* court as a legally cognizable "species of trade name" in which an individual had an exploitable commercial interest.[28] In this sense, right of publicity sounds more like trademark than it does like privacy.

In contrast to this economic framing, courts sometimes ground the right of publicity in terms of a person's interest in controlling their own identity. Underlying this privacy-based rationale are concerns regarding the "natural rights" to human identity and allowing individuals to exert their own personal agency by retaining control over their representation in the public sphere.[29] This interpretation makes the right of publicity a "right of self-definition," as it prohibits unauthorized uses of an individual's identity that might "interfere with the meaning and values the public associates with that person."[30]

Courts and scholars have more frequently adopted the economic framing, however, conceiving of the right of publicity as a vehicle for protecting an individual's opportunities to profit from the commercial value of their identity.[31] This economic approach construes the commercial value derived from one's identity as a type of "property," accompanied by corresponding exclusionary rights. Under this theory, personal identity is a scarce resource, and recognition of identity as a property right is justified by the economic interest in ensuring the best and most efficient way of allocating resources. Absent the promise of an "exclusive grant" in a commercially exploitable identity, "many prominent persons . . . would feel sorely deprived,"[32] and perhaps less inclined to participate in public life in a manner that would cause them to attain social prominence.[33]

Right of publicity is a creature of state law, with each jurisdiction having a slightly different regime.[34] A handful of states, including most notably New York and California, have enacted statutes codifying the right of publicity. Others rely on common law. Despite this rag-tag approach, right of publicity actions tend to share common elements. Central to the cause of action are nonconsensual use of the plaintiff's identity, commercial exploitation, and resulting injury. But states vary when they set the precise contours of the right. States differ in their requirements for who specifically can invoke the right; whether they recognize post-mortem publicity rights; and acceptable exceptions and affirmative defenses. This raises hard conflicts of law questions.

---

[27] *Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc.*, 202 F.2d 866, 868 (2d Cir. 1953); Daniel Gervais and Martin L. Holmes, *Fame, Property & Identity: The Purpose and Scope of the Right of Publicity,* 25 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 181, 188 (2014).

[28] *Motschenbacher v. R.J. Reynolds Tobacco Co*, 498 F.2d 821, 825 (9th Cir. 1974).

[29] J. Thomas McCarthy, *The Rights of Publicity and Privacy* § 2:2 (2d ed. 2023).

[30] *Id*. at § 2:9

[31] *See, e.g., Gionfriddo v. Major League Baseball*, 94 Cal.App.4th 400, 408 (2001); Richard Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 411–414 (1978).

[32] *Haelan*, 202 F.2d at 868.

[33] *See* McCarthy, *supra* note 29, at § 2:6.

[34] For those interested in the law of a particular state, consider: Jennifer E. Rothman, *Right of Publicity State-by-State* at http://www.rightofpublicityroadmap.com/.

California and New York offer useful models for understanding the right of publicity. California recognizes the right of publicity under both common law and state statute. Sections 3344 and 3344.1 of the California Civil Code govern right of publicity among living and deceased persons, respectively.[35] To succeed in a common law cause of action in California, a plaintiff must prove: "(1) the defendant's use of the plaintiff's identity; (2) the appropriation of plaintiff's name or likeness to defendant's advantage, commercially or otherwise; (3) lack of consent; and (4) resulting injury."[36] Statutory causes of action require the additional elements of "knowing use" of the plaintiff's identity in direct connection with a "commercial purpose."[37]

New York, alternatively, allows only statutory right of publicity claims through sections 50 and 51 of New York Civil Rights Law. Section 50 renders it a misdemeanor to use of "the name, portrait, picture, likeness, or voice of any living person without having first obtained the written consent of such a person" for either "advertising purposes, or for the purposes of trade" by "any person, firm or corporation," while section 51 creates an analogous private right of action.

New York's statutory right of publicity claims under sections 50 and 51 are broad, extending to celebrities and non-celebrities alike.[38] The statute does include exceptions, however, including those for literary works, television, and audio works; parody; and satire. The recently passed section 50-F is more limited. The statutory provision covers only "deceased performers" and "deceased personalities" who were domiciled in the state at the time of their death and "regularly engaged in acting, singing, dancing, or playing a musical instrument" (deceased performers) or "whose name, voice, signature, photograph, or likeness has commercial value at the time of his or her death" (deceased personalities). The statute is replete with exceptions, including those where the use is connected with a "literary work; musical work or composition; work of art or other visual work; work of political, public interest, educational or newsworthy value . . . audio or audiovisual work, radio or television program . . . ." It also includes works of "parody, satire, commentary or criticism, . . . political or newsworthy value, or similar works, . . . a representation of a deceased performer as [themselves] . . . except in a live performance of a musical word, de minimus or incidental [use]," as well as "in connection with any news, public affairs or sports program or account . . . or any political campaign."

Despite the differences between New York and California in theory, there are substantial commonalities in effect. Across jurisdictions, the "name or likeness requirement" has been interpreted broadly to include any type of "indicia of identity" so long as it is distinctive, including voice and personal style. The likeness need not be a literal depiction of an individual so long as the depiction renders the individual recognizable. The definitions of "commercial advantage" and "advertising purposes or for the purpose of trade" have also both been broadly construed, with courts defining these types of appropriation as any use intended to gain an audience's attention. Yet differences do emerge once cases move away from direct advertising to more expressive uses. To avoid running afoul of the First Amendment, many states create either an exception or an affirmative defense regarding uses that are in the public

---

[35] *Right of Publicity: Overview*, Westlaw Practical Law Intellectual Property & Technology.

[36] *White v. Samsung Electronics America, Inc.*, 971 F.2d 1395, 1397 (9th Cir. 1992).

[37] Cal. Civ. Code § 3344; Cal. Civ. Code § 3344(a)("Knowing use" is defined as an individual's "name, voice, signature, photograph or likeness." "Commercial purposes" include: use "on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services.").

[38] *See Stephano v. News Grp. Publ'ns, Inc.*, 64 N.Y.2d 174, 182 (1984) ("Section 51 of the Civil Rights Law has been applied in cases . . . where the picture of a person who has apparently never sought publicity has been used without his or her consent for trade or advertising purposes.").

interest or are otherwise expressive works. But the details of these exceptions vary markedly across jurisdictions.[39]

White v. Samsung Electronics America, Inc. 971 F.2d 1395 (9th Cir. 1992)

GOODWIN, Senior Circuit Judge:

This case involves a promotional "fame and fortune" dispute. In running a particular advertisement without Vanna White's permission, defendants Samsung Electronics America, Inc. (Samsung) and David Deutsch Associates, Inc. (Deutsch) attempted to capitalize on White's fame to enhance their fortune. White sued, alleging infringement of various intellectual property rights, but the district court granted summary judgment in favor of the defendants.

Plaintiff Vanna White is the hostess of "Wheel of Fortune," one of the most popular game shows in television history. An estimated forty million people watch the program daily. Capitalizing on the fame which her participation in the show has bestowed on her, White markets her identity to various advertisers.

The dispute in this case arose out of a series of advertisements prepared for Samsung by Deutsch. The series ran in at least half a dozen publications with widespread, and in some cases national, circulation. Each of the advertisements in the series followed the same theme. Each depicted a current item from popular culture and a Samsung electronic product. Each was set in the twenty-first century and conveyed the message that the Samsung product would still be in use by that time. By hypothesizing outrageous future outcomes for the cultural items, the ads created humorous effects. For example, one lampooned current popular notions of an unhealthy diet by depicting a raw steak with the caption: "Revealed to be health food. 2010 A.D." Another depicted irreverent "news"-show host Morton Downey Jr. in front of an American flag with the caption: "Presidential candidate. 2008 A.D."

The advertisement which prompted the current dispute was for Samsung video-cassette recorders (VCRs). The ad depicted a robot, dressed in a wig, gown, and jewelry which Deutsch consciously selected to resemble White's hair and dress. The robot was posed next to a game board which is instantly recognizable as the Wheel of Fortune game show set, in a stance for which White is famous. The caption of the ad read: "Longest-running game show. 2012 A.D." Defendants referred to the ad as the "Vanna White" ad. Unlike the other celebrities used in the campaign, White neither consented to the ads nor was she paid.

Following the circulation of the robot ad, White sued Samsung and Deutsch in federal district court under: (1) California Civil Code § 3344; (2) the California common law right of publicity; and (3) § 43(a) of the Lanham Act, 15 U.S.C. § 1125(a). The district court granted summary judgment against White on each of her claims. White now appeals.

I. Section 3344

White first argues that the district court erred in rejecting her claim under section 3344. Section 3344(a) provides, in pertinent part, that "[a]ny person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, . . . for purposes of advertising or selling, . . . without such person's prior consent . . . shall be liable for any damages sustained by the person or persons injured as a result thereof."

White argues that the Samsung advertisement used her "likeness" in contravention of section 3344. In *Midler v. Ford Motor Co.* (9th Cir. 1988), this court rejected Bette Midler's section 3344 claim concerning a Ford television commercial in which a Midler "sound-alike" sang a song which Midler had made famous. In rejecting Midler's claim, this court noted that "[t]he defendants did not use Midler's name or anything else whose use is prohibited by the

[39] See, e.g., Alice Preminger and Matthew B. Kugler, *The Right of Publicity Can Save Actors from Deepfake Armageddon*, 39 BERKELEY TECH. L.J. 783, 795–797 (2024).

statute. The voice they used was [another person's], not hers. The term 'likeness' refers to a visual image not a vocal imitation."

In this case, Samsung and Deutsch used a robot with mechanical features, and not, for example, a manikin molded to White's precise features. Without deciding for all purposes when a caricature or impressionistic resemblance might become a "likeness," we agree with the district court that the robot at issue here was not White's "likeness" within the meaning of section 3344. Accordingly, we affirm the court's dismissal of White's section 3344 claim.

II. Right of Publicity

White next argues that the district court erred in granting summary judgment to defendants on White's common law right of publicity claim. In *Eastwood v. Superior Court,* (1983), the California court of appeal stated that the common law right of publicity cause of action "may be pleaded by alleging (1) the defendant's use of the plaintiff's identity; (2) the appropriation of plaintiff's name or likeness to defendant's advantage, commercially or otherwise; (3) lack of consent; and (4) resulting injury." The district court dismissed White's claim for failure to satisfy *Eastwood's* second prong, reasoning that defendants had not appropriated White's "name or likeness" with their robot ad. We agree that the robot ad did not make use of White's name or likeness. However, the common law right of publicity is not so confined.

The *Eastwood* court did not hold that the right of publicity cause of action could be pleaded only by alleging an appropriation of name or likeness. *Eastwood* involved an unauthorized use of photographs of Clint Eastwood and of his name. Accordingly, the *Eastwood* court had no occasion to consider the extent beyond the use of name or likeness to which the right of publicity reaches. That court held only that the right of publicity cause of action "may be" pleaded by alleging, *inter alia,* appropriation of name or likeness, not that the action may be pleaded *only* in those terms.

The "name or likeness" formulation referred to in *Eastwood* originated not as an element of the right of publicity cause of action, but as a description of the types of cases in which the cause of action had been recognized. The source of this formulation is Prosser, *Privacy* (1960), one of the earliest and most enduring articulations of the common law right of publicity cause of action. In looking at the case law to that point, Prosser recognized that right of publicity cases involved one of two basic factual scenarios: name appropriation, and picture or other likeness appropriation.

Even though Prosser focused on appropriations of name or likeness in discussing the right of publicity, he noted that "[i]t is not impossible that there might be appropriation of the plaintiff's identity, as by impersonation, without the use of either his name or his likeness, and that this would be an invasion of his right of privacy." At the time Prosser wrote, he noted however, that "[n]o such case appears to have arisen."

Since Prosser's early formulation, the case law has borne out his insight that the right of publicity is not limited to the appropriation of name or likeness. In *Motschenbacher v. R.J. Reynolds Tobacco Co.* (9th Cir. 1974), the defendant had used a photograph of the plaintiff's race car in a television commercial. Although the plaintiff appeared driving the car in the photograph, his features were not visible. Even though the defendant had not appropriated the plaintiff's name or likeness, this court held that plaintiff's California right of publicity claim should reach the jury.

In *Midler,* this court held that, even though the defendants had not used Midler's name or likeness, Midler had stated a claim for violation of her California common law right of publicity because "the defendants . . . for their own profit in selling their product did appropriate part of her identity" by using a Midler sound-alike.

In *Carson v. Here's Johnny Portable Toilets, Inc.* (6th Cir. 1983), the defendant had marketed portable toilets under the brand name "Here's Johnny"—Johnny Carson's signature "Tonight Show" introduction—without Carson's permission. The district court had dismissed Carson's Michigan common law right of publicity claim because the defendants had not used Carson's "name or likeness." In reversing the district court, the sixth circuit found "the district court's conception of the right of publicity . . . too narrow" and held that the right was implicated because the defendant had appropriated Carson's identity by using, *inter alia,* the phrase "Here's Johnny."

These cases teach not only that the common law right of publicity reaches means of appropriation other than name or likeness, but that the specific means of appropriation are relevant only for determining whether the defendant has in fact appropriated the plaintiff's identity. The right of publicity does not require that appropriations of identity be accomplished through particular means to be actionable. It is noteworthy that the *Midler* and *Carson* defendants not only avoided using the plaintiff's name or likeness, but they also avoided appropriating the celebrity's voice, signature, and photograph. The photograph in *Motschenbacher* did include the plaintiff, but because the plaintiff was not visible the driver could have been an actor or dummy and the analysis in the case would have been the same.

Although the defendants in these cases avoided the most obvious means of appropriating the plaintiffs' identities, each of their actions directly implicated the commercial interests which the right of publicity is designed to protect. As the *Carson* court explained:

> [t]he right of publicity has developed to protect the commercial interest of celebrities in their identities. The theory of the right is that a celebrity's identity can be valuable in the promotion of products, and the celebrity has an interest that may be protected from the unauthorized commercial exploitation of that identity . . . . If the celebrity's identity is commercially exploited, there has been an invasion of his right whether or not his "name or likeness" is used.

It is not important *how* the defendant has appropriated the plaintiff's identity, but *whether* the defendant has done so. *Motschenbacher, Midler,* and *Carson* teach the impossibility of treating the right of publicity as guarding only against a laundry list of specific means of appropriating identity. A rule which says that the right of publicity can be infringed only through the use of nine different methods of appropriating identity merely challenges the clever advertising strategist to come up with the tenth.

Indeed, if we treated the means of appropriation as dispositive in our analysis of the right of publicity, we would not only weaken the right but effectively eviscerate it. The right would fail to protect those plaintiffs most in need of its protection. Advertisers use celebrities to promote their products. The more popular the celebrity, the greater the number of people who recognize her, and the greater the visibility for the product. The identities of the most popular celebrities are not only the most attractive for advertisers, but also the easiest to evoke without resorting to obvious means such as name, likeness, or voice.

Consider a hypothetical advertisement which depicts a mechanical robot with male features, an African–American complexion, and a bald head. The robot is wearing black hightop Air Jordan basketball sneakers, and a red basketball uniform with black trim, baggy shorts, and the number 23 (though not revealing "Bulls" or "Jordan" lettering). The ad depicts the robot dunking a basketball one-handed, stiff-armed, legs extended like open scissors, and tongue hanging out. Now envision that this ad is run on television during professional basketball games. Considered individually, the robot's physical attributes, its dress, and its stance tell us little. Taken together, they lead to the only conclusion that any sports viewer who has registered a discernible pulse in the past five years would reach: the ad is about Michael Jordan.

Viewed separately, the individual aspects of the advertisement in the present case say little. Viewed together, they leave little doubt about the celebrity the ad is meant to depict. The

female-shaped robot is wearing a long gown, blond wig, and large jewelry. Vanna White dresses exactly like this at times, but so do many other women. The robot is in the process of turning a block letter on a game-board. Vanna White dresses like this while turning letters on a game-board but perhaps similarly attired Scrabble-playing women do this as well. The robot is standing on what looks to be the Wheel of Fortune game show set. Vanna White dresses like this, turns letters, and does this on the Wheel of Fortune game show. She is the only one. Indeed, defendants themselves referred to their ad as the "Vanna White" ad. We are not surprised.

Television and other media create marketable celebrity identity value. Considerable energy and ingenuity are expended by those who have achieved celebrity value to exploit it for profit. The law protects the celebrity's sole right to exploit this value whether the celebrity has achieved her fame out of rare ability, dumb luck, or a combination thereof. We decline Samsung and Deutch's invitation to permit the evisceration of the common law right of publicity through means as facile as those in this case. Because White has alleged facts showing that Samsung and Deutsch had appropriated her identity, the district court erred by rejecting, on summary judgment, White's common law right of publicity claim.

IV. The Parody Defense

In defense, defendants cite a number of cases for the proposition that their robot ad constituted protected speech. The only cases they cite which are even remotely relevant to this case are *Hustler Magazine v. Falwell* (1988) and *L.L. Bean, Inc. v. Drake Publishers, Inc.* (1st Cir. 1987). Those cases involved parodies of advertisements run for the purpose of poking fun at Jerry Falwell and L.L. Bean, respectively. This case involves a true advertisement run for the purpose of selling Samsung VCRs. The ad's spoof of Vanna White and Wheel of Fortune is subservient and only tangentially related to the ad's primary message: "buy Samsung VCRs." Defendants' parody arguments are better addressed to non-commercial parodies. The difference between a "parody" and a "knock-off" is the difference between fun and profit.

Notes

1. The most conventional right of publicity case involves the nonconsensual use of a person's likeness in an advertisement. This will almost always count as a use for purposes of trade/commercial advantage. And, as *White* shows, likeness is often defined broadly.
2. Expressive uses are often outside the scope of right of publicity statutes either under a statutory exception or because they are protected by the First Amendment. A court assessing an expressive use claim might use any of several different tests. The most commonly employed test considers whether an unauthorized appropriation of likeness is sufficiently "transformative."[40] A court fundamentally asks, "whether a product containing a celebrity's likeness is so transformed that it has become primarily the defendant's own expression rather than the celebrity's likeness."[41] In short, is this a picture of Barack Obama, or is it a work of the artist? This test may have a family resemblance to the transformative use test in copyright law, but is distinct.

   In the Ninth Circuit, this transformative use test is comprised of five inquiries.[42] First, whether "the celebrity likeness is one of the 'raw materials' from which an original work is synthesized." If not, the rest of the test is not considered relevant. Second, whether the work "is primarily the defendant's own expression . . . [and also is expression of] something other than the likeness of the celebrity." Third, "whether [quantitatively] the literal and imitative

[40] *Comedy III Productions v. Gary Saderup*, 21 P.3d 797, 808 (Cal. 2001).

[41] *Id.* at 809.

[42] *In re NCAA Student-Athlete Name & Likeness Licensing Litigation*, 724 F.3d 1268, 1274 (9th Cir. 2013). See also *Hamilton v. Speight*, 827 F. App'x 238, 240 (3d Cir. 2020) for application of transformative use test by the Third Circuit, and *Comedy III*, 21 P.3d at 809 for application of the transformative use test by the California Supreme Court.

or creative elements predominate in the work." Fourth, whether "the marketability and economic value of the challenged work derive primarily from the fame of the celebrity depicted." Finally, the work is deemed less likely to be transformative if "an artist's skill and talent is manifestly subordinated to the overall goal of creating a conventional portrait of a celebrity so as to commercially exploit his or her fame." Making a movie about a person will often count as an expressive use under this test. Using them to sell sunscreen will not count as an expressive use. Using them as a model for a character in a video game will often not count as an expressive use, but this is one of the hotter and more complex areas of right of publicity law.

One emerging issue in right of publicity law involves the use of deepfake videos. Previously, impersonations of individuals were limited by technology. If one wanted Vanna White to appear to endorse a product or make a statement, then one needed to either: 1.) hire Vanna White, 2.) hire a convincing Vanna White impersonator, or 3) do something more symbolic, as did Samsung with its Vanna White robot. Now it is possible to use computer imagery to make take a video of someone else saying a message or performing an action and to substitute in a realistic facsimile of Vanna White. To date, this has mostly been an issue for nonconsensual pornography (see Chapter 2.E, below). But there is substantial concern that such deepfake technology will change the non-pornographic portions of the entertainment industry as well.

In a 2024 article, Alice Preminger and Matthew Kugler reviewed the state of right of publicity law as it relates to deepfakes.[43] They differentiated between three possible uses of deepfakes: deepfakes to sell products, deepfakes as products, and deepfakes as noncommercial expression. In their view, the use of deepfakes to sell products was easily handled under traditional right of publicity law, as in the *White* case. The deepfake is simply a new way of appropriating identity. The use of deepfakes as products – where the deepfake itself is the thing being sold – is somewhat more complicated. In a way, it is parallel to selling dolls of a person, which would often count as a violation of their right of publicity. But it also can sometimes implicate First Amendment expressive protections. The below *Young v. NeoCortext* case is one of the first to grapple with this issue.

As one considers the *Young* case, it is important to keep in mind the third set of deepfake uses: deepfakes as a form of noncommercial expression. People have made deepfake videos in the course of performing political commentary, and for simple amusement. These are generally not sold and are not commercial (except in the most indirect way). For example, a deepfake video was made of former President Obama calling then-President Donald Trump a "dipshit" as part of a public service announcement regarding deepfakes.[44] Others have featured political figures playing games and trash talking each other.[45] As right of publicity law considers deepfakes, it is important to balance both their commercial impact as well as their role in this type of political expression.

Young v. NeoCortext, Inc., 690 F. Supp. 3d 1091 (C.D. Cal. 2023)

Wesley L. Hsu United States District Judge

This is a putative class action. Defendant NeoCortext is the developer of the "Reface" application. Users may download Reface to their smartphone through the Apple App Store or

---

[43] Alice Preminger and Matthew B. Kugler, *The Right of Publicity Can Save Actors from Deepfake Armageddon*, 39 BERKELEY TECH. L.J. 783 (2024).

[44] James Vincent, *Watch Jordan Peele Use AI to Make Barack Obama Deliver a PSA About Fake News,* VERGE (Apr. 17, 2018), https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed.

[45] Tmparagon, *Trump Plays Destiny with Biden and Obama*, TIKTOK (Feb. 19, 2023), https://www.tiktok.com/@tmparagon/video/7202039315461917994.

the Google Play Store. Reface "allows users to swap their faces with actors, musicians, athletes, celebrities, and other well-known individuals in scenes from popular shows, movies, and other short-form internet media." The application contains a "Pre-sets" catalogue containing images and videos of different celebrities compiled from a variety of websites. The catalogue is searchable and allows users to find specific individuals to swap faces with. Once a user has selected an individual, she may upload an image to Reface from her smartphone. The application then identifies the faces in the photographs and generates a new image, swapping the face of the celebrity for that of the person in the user-uploaded image. In that way, according to the marketing for Reface, the user can "choose who [they would] like to become."

NeoCortext offers both free and "PRO" versions of Reface. With the free version of Reface, the user-generated face-swapped image is watermarked with text that says "made with reface app." Below the generated image is a button showing a crossed-out water drop symbol. If the user hits that button, they are prompted to pay for a PRO subscription at $5.99 for a week or $36.99 for a lifetime. With Reface PRO, face-swapped images are not watermarked.

Plaintiff Kyland Young is a cast member of several reality television shows, including the CBS show Big Brother. The Reface Pre-sets catalogue contains videos and images of Young from Big Brother. Plaintiff alleges that Defendant "was using his identity to solicit the purchase of paid subscriptions to the Reface application" and that "[t]here are several animated images depicting Mr. Young on the Reface application, which Free and PRO Users can manipulate to become him." Young did not consent to NeoCortext's use of his image in the Reface application, and he has never received compensation for the use of his image in the Reface application. Nevertheless, he says, NeoCortext profits from using his likeness in the Reface application.

Young is suing NeoCortext for violation of the right of publicity under California Civil Code section 3344. Young alleges that the watermarked images created with the free version of Reface are "teasers," and that the watermarks "incentivize users to pay to remove them" and "serve as free advertising to attract new downloads of the Reface application." He also alleges that the images generated with the PRO version of Reface are "paid product[s]" that "constitute[ ] commercial use and purpose." Therefore, he alleges, NeoCortext "us[es] his identity to solicit the purchase of paid subscriptions to the Reface application." Young seeks to represent a class of "California residents whose name, voice, signature, photograph, or likeness was displayed on a Reface application Teaser Face Swap or the PRO Version of the Reface application on or after April 3, 2021," three years before he filed the Complaint.

NeoCortext moves to dismiss Young's single cause of action under Federal Rule of Civil Procedure 12(b)(6). It also brings a special motion to strike under California's anti-SLAPP statute, California Code of Civil Procedure section 425.16

Under California's "anti-SLAPP" law,[1] California Code of Civil Procedure section 425.16, defendants may move to strike "actions. that masquerade as ordinary lawsuits but are intended to deter ordinary people from exercising their political or legal rights or to punish them for doing so." Importantly, "[t]he anti-SLAPP statute does not insulate defendants from any liability for claims arising from the protected rights of petition or speech. It only provides a procedure for weeding out, at an early stage, meritless claims arising from protected activity." *Baral v. Schnitt*, 1 Cal. 5th 376, 384 (2016).

Deciding an anti-SLAPP motion involves two steps. First, the court must determine "whether the defendant has made a threshold showing that the challenged cause of action is one arising from protected activity." That is, the defendant must show that the conduct underlying the case was done "in furtherance of the [defendant's] right of petition or free speech under the United States Constitution or the California Constitution in connection with a public issue." Cal. Civ. Proc. Code § 425.16.

[1] The "SLAPP" in anti-SLAPP stands for "strategic lawsuit against public participation."

If the court finds the defendant has made such a showing, it proceeds to the second step: determining "whether the plaintiff has demonstrated a probability of prevailing on the claim." On this second step, "[t]he court does not weigh evidence or resolve conflicting factual claims." *Baral*. Rather,

> [i]ts inquiry is limited to whether the plaintiff has stated a legally sufficient claim and made a prima facie factual showing sufficient to sustain a favorable judgment. It accepts the plaintiff's evidence as true, and evaluates the defendant's showing only to determine if it defeats the plaintiff's claim as a matter of law. Claims with the requisite minimal merit may proceed.

Baral. In other words, if the defendant does not prevail as a matter of law, the plaintiff's claim survives the defendant's anti-SLAPP motion to strike.

Because the standard on step two of anti-SLAPP is identical to that on a Rule 12(b)(6) motion, the Court begins with the anti-SLAPP analysis.

A. Anti-SLAPP Step One

To clear the first hurdle, NeoCortext must show that the "act underlying the plaintiff's cause of action" was "itself. an act in furtherance of the right of petition or free speech." Here, "the focus is on determining what the defendant's activity is that gives rise to his or her asserted liability—and whether that activity constitutes protected speech or petitioning" under the anti-SLAPP statute.

As defined in the anti-SLAPP statute, an "act in furtherance of a person's right of petition or free speech" includes "conduct in furtherance of the exercise of the constitutional right of petition or the constitutional right of free speech." Cal. Civ. Proc. Code § 425.16(e). That is, "the statute's reach is not restricted to speech, but expressly applies to conduct." Importantly, "that conduct is not limited to the exercise of [the defendant's] right of free speech, but to all conduct in furtherance of the exercise of the right of free speech."

The conduct that forms the basis of Young's Complaint is NeoCortext's inclusion of Young's name and image in the Reface app, and the invitation for users to combine their image with Young's to create a new, third image. As the conduct is described in the Complaint, the users—not NeoCortext—exercise their free speech rights when they use Reface to create new images. The question, therefore, is whether NeoCortext's use of Young's image in its application is conduct taken in furtherance of users' exercise of free speech.

As the Ninth Circuit has recognized, California courts "have interpreted this piece of the defendant's threshold showing rather loosely." For example, in *Tamkin v. CBS Broadcasting, Inc.*, 193 Cal. App. 4th 133 (2011), a television writer drafted a script that used plaintiffs' names as placeholders for two unsympathetic characters, and the network that aired the show approved the dissemination of the draft script for casting purposes. Even though the characters' names changed by the time the episode was filmed, the plaintiffs sued both the writer and the network for defamation based on the original script. The court found that the writer's creation of the draft and the network's approval of its dissemination constituted conduct in furtherance of the exercise of free speech because they "helped to advance or assist in the creation, casting, and broadcasting of an episode of a popular television show." That is, even though the allegedly defamatory material did not ultimately end up in the "speech"—the episode of the television show—the material assisted in the creation of the speech, and therefore was "in furtherance" of it.

One might argue that the user-generated images that constitute the "speech" in this case do not implicate the same high-level free speech concerns as the cases above. But at this step, the "inquiry does not turn on a normative evaluation of the substance of the speech," and the Court is "not concerned with the social utility of the speech at issue, or the degree to which it propelled the conversation in any particular direction." Indeed, "because celebrities take on

personal meanings to many individuals. the creative appropriation of celebrity images can be an important avenue of individual expression." Wrongful or not, NeoCortext's use of Young's image gives users a tool for such expression. It is therefore "conduct in furtherance of" users' free speech rights.

The next inquiry is whether NeoCortext has shown that the speech its conduct furthers is connected with a "public issue." Cal. Civ. Proc. Code § 425.16. While there is no definitive test for what constitutes a "public issue," under one widely used test, a public issue may fall under three categories: "(1) statements concerning a person or entity in the public eye; (2) conduct that could directly affect a large number of people beyond the direct participants; (3) or a topic of widespread, public interest." Young, as a reality show cast member, is in the public eye. NeoCortext's conduct—using celebrities' likenesses in the Reface application—could directly affect many people whose images might also be used. Finally, the use of technology to alter images and videos of individuals in a way that makes them look realistic is a topic of widespread public interest. Young does not dispute any of this.

Because NeoCortext has shown that its conduct is in furtherance of the right of free speech made in connection with a public issue, it has satisfied its burden on the first step of the anti-SLAPP analysis.

B. Anti-SLAPP Step Two and 12(b)(6)

As discussed above, when a defendant carries its burden on the first step of the anti-SLAPP analysis, the burden then shifts to the plaintiff to show "a probability of prevailing on the claim." Cal. Civ. Proc. Code § 425.16. NeoCortext argues that Young has not done so for three reasons. First, NeoCortext argues that Young's right of publicity claim is preempted by the Copyright Act. Second, NeoCortext argues that the claim is barred by the First Amendment. Finally, NeoCortext asserts that Young has not made a prima facie showing that NeoCortext violated his right of publicity. The Court addresses each argument in turn.

1. Copyright Preemption

The Copyright Act "preempt[s] and abolish[es] any rights under the common law or statutes of a State that are equivalent to copyright" and that fall "within the scope of the Federal copyright law."

While the Copyright Act protects ownership of photographs, it does not protect the exploitation of one's likeness—even if it is embodied in a photograph. The photograph itself, as a pictorial work of authorship, is subject matter protected by the Copyright Act. However, it is not the publication of the photograph itself, as a creative work of authorship, that is the basis for Appellants' claims, but rather, it is the use of the Appellants' likenesses and their names pictured in the published photograph.

[The Ninth Circuit] said that precedent "implies that misuse of an individual's likeness is the basis of a publicity-right claim when the name or image is exploited in advertising or on merchandise." On the other hand, the court said, "one's likeness does not form the basis of a publicity-right claim when the tort action challenges control of the artistic work itself or involves the mere republication of the photograph."

Young's right of publicity claim does not fall within the subject matter of copyright. Like the plaintiffs in Downing, Young does not challenge the control of the images used in the Reface application, nor is his complaint about the "mere republication" of those images. Rather, the basis of Young's claim is that NeoCortext uses his likeness on advertising and merchandise when it allows users to create a product containing his image.

Although not binding on this Court, the Court does find the analysis in *Bonilla v. Ancestry.com Operations Inc.* (N.D. Ill. 2021), persuasive. While not identical to this case, that court distinguished *Maloney* when denying a motion to dismiss where the defendant used the

plaintiff's copyrighted yearbook photograph to advertise the defendant's website's services. Thus, Bonilla too supports this Court's conclusion.

Because Young's allegations center on how his name and likeness are used in NeoCortext's products and not on the ownership rights to the images themselves, Young's claim in the Complaint does not fall under the subject-matter of copyright, and his claim is therefore not preempted under the Copyright Act.

For the same reasons as set forth in the above analysis as to preemption, the Court finds that, on the face of the Complaint, the rights Young asserts here are not equivalent to the rights conferred by the Copyright Act to the owners of the photographs at issue. Section 106 of the Copyright Act does not confer upon the owners of the photographs the right to use Young's name and various likenesses to advertise the free version of its software—a product intended to lead to purchases of subscriptions to its full product. Young is not seeking to "merely" restrict the reproduction or distribution of the original photographs/works, as the plaintiffs in Maloney and Laws. Therefore, this second factor also fails.

2. First Amendment Transformative Use

Under California law, "when an artist is faced with a right of publicity challenge to his or her work, he or she may raise as [an] affirmative defense that the work is protected by the First Amendment inasmuch as it contains significant transformative elements or that the value of the work does not derive primarily from the celebrity's fame." *Comedy III Prods. V. Saderup* (Cal. 2001). This inquiry hinges on "whether the celebrity likeness is one of the 'raw materials' from which an original work is synthesized, or whether the depiction or imitation of the celebrity is the very sum and substance of the work in question."

At this stage, to defeat Young's claim, NeoCortext must show that its use is transformative as a matter of law. NeoCortext argues that it has done so because "[t]he very purpose of Reface is to transform a photo or video in which Plaintiff's (or others) [sic] image appears into a new work in which Plaintiff's face does not appear." But Young's face is the only thing that changes in the end product; at least in some instances, the end photograph still depicts the rest of Young's body in the setting in which he became a celebrity.

The Ninth Circuit has found that depictions that are arguably more transformative than those created with Reface do not entitle a defendant to the affirmative defense as a matter of law. For example, in *Hilton*, the Ninth Circuit considered a greeting card depicting Paris Hilton as a waitress and using her signature catch phrase. The picture was taken from an episode of a reality television show in which Hilton worked as a waitress. The Ninth Circuit pointed out that "there are some differences between the waitressing Hilton does in the. episode and the portrayal in Hallmark's card," including the style of the restaurant, Hilton's uniform, and the food. Additionally, "the body underneath Hilton's over-sized head [was] a cartoon drawing of a generic female body rather than a picture of Hilton's real body." "Despite these differences," the court found, "the basic setting is the same: we see Paris Hilton, born to privilege, working as a waitress." The Ninth Circuit thus found that Hallmark was not entitled to the transformative use defense as a matter of law.

NeoCortext's reliance on *Winter v. D.C. Comics Inc* (Cal. 2003), and *Kirby v. Sega of Am., Inc.,* (Cal. App. 2006), is unavailing. Both of those cases involved artistic renditions of the plaintiffs—in Winter for comic books and in Kirby for video games. Here, the replacement of Young's face on an actual photograph of Young is not "transformative" in the manner asserted in *Winter* and *Kirby*. Indeed, the whole point of NeoCortext's product is to ensure that the image of Young is not so transformed that it reduces the "shock value" of the user's face on Young's body in a recognizable situation. Also of note, both *Winter* and *Kirby* were decided at the summary judgment stage when an evidentiary record had been developed, not at the motion to dismiss stage.

The replacement of Young's face in the Reface application is most analogous to the replacement of Hilton's body in the greeting card at issue in *Hilton* or the use of computer-generated images of athletes in a sports video game as in *In re NCAA Student-Athlete*. While it may ultimately be deemed transformative as a matter of fact, that does not entitle NeoCortext to the defense as a matter of law. NeoCortext has therefore not shown that the First Amendment bars Young's right of publicity claim.

3. Prima Facie Showing

A right of publicity claim under California Civil Code section 3344, like the one Young brings here, requires a plaintiff to establish (1) defendant's knowing use of the plaintiff's identity; (2) "the appropriation of plaintiff's name or likeness to defendant's advantage, commercially or otherwise"; (3) "a direct connection between the alleged use and the commercial purpose"; (4) a lack of consent; and (5) a resulting injury.

NeoCortext's main argument here is that Young has not established that NeoCortext "knowingly" used Young's identity in the Reface application. For his part, Young argues that his allegations lead to the reasonable inference that NeoCortext acted knowingly by "programm[ing] an app that scraped video clips of him, indexed him in its database, permitted him to be searchable through the [application's] search bar, and allowed users to become him."

NeoCortext does not provide support for its apparent assertion that "knowingly" means "with affirmative knowledge of" the presence of Young's image in the Reface application. Construing the Complaint in the light most favorable to Young, the Court finds that Young has adequately pled that NeoCortext "knowingly" used his identity when it compiled his images with his name in the Reface application and made the images available for users to manipulate.

For the reasons stated above, NeoCortext's Motion to Dismiss and Motion to Strike are DENIED.

Notes

1. This decision was affirmed in a brief opinion on appeal, *Young v. NeoCortext, Inc.*, No. 23-55772, 2024 WL 4987254 (9th Cir. Dec. 5, 2024).
2. The alleged bad conduct in this case goes beyond merely making a tool to swap faces. NeoCortext was alleged to have created a stable of celebrities whose faces were subject to replacement. The inclusion of Young's face and body in that stable appears to have been intentional, so the use of his identity was likewise intentional.
3. In their review of deepfakes and the right of publicity, Preminger and Kugler state "The ability to create deepfakes represents the next quantum leap in the potential to easily appropriate another's likeness in a manner that profoundly undermines both the economic and reputational interests that right of publicity law seeks to protect."[46] To what extent are they correct? Is a deepfake of Vanna White more impactful than the robotic depiction of the 1990s? Should policymakers be concerned about the possibility of replacing live actors with computer-simulated doppelgangers? What about Cameo-style videos, where actors and public figures are paid to record personalized messages?

[46] Alice Preminger and Matthew B. Kugler, *The Right of Publicity Can Save Actors from Deepfake Armageddon*, 39 BERKELEY TECH. L.J. 783, 839 (2024).

E. Nonconsensual pornography and image-based sexual abuse

Every state now has a law restricting the nonconsensual dissemination of some intimate images and videos. These laws began to be passed in the 2010s in response to growing awareness of the harms of what was then called "revenge porn." These laws have been repeatedly challenged on First Amendment grounds but, as of 2024, every state supreme court to consider these laws has upheld them. The below case from the Vermont Supreme Court is typical in both its analysis and conclusions. It concerns three actors: the complainant, whose image was shared; Mr. Coon, the complainant's prospective love interest; and the defendant, VanBuren, who also had some relationship with Mr. Coon. Note its extensive citations to the work of Mary Anne Franks and Danielle Citron, two legal scholars who were at the forefront of the campaign to pass these laws.

State v. VanBuren, 214 A.3d 791 (Vt. 2019)

ROBINSON, J.

This case raises a facial challenge to Vermont's statute banning disclosure of nonconsensual pornography. 13 V.S.A. § 2606. We conclude that the statute is constitutional on its face and grant the State's petition for extraordinary relief.

I. "Revenge-Porn," or Nonconsensual Pornography Generally

"Revenge porn" is a popular label describing a subset of nonconsensual pornography published for vengeful purposes. "Nonconsensual pornography" may be defined generally as "distribution of sexually graphic images of individuals without their consent." D. Citron & M. Franks, *Criminalizing Revenge Porn*, 49 Wake Forest L. Rev. 345, 346 (2014). The term "nonconsensual pornography" encompasses "images originally obtained without consent (e.g., hidden recordings or recordings of sexual assaults) as well as images originally obtained with consent, usually within the context of a private or confidential relationship." The nonconsensual dissemination of such intimate images—to a victim's employer, coworkers, family members, friends, or even strangers—can cause "public degradation, social isolation, and professional humiliation for the victims." C. Alter, "'It's Like Having an Incurable Disease': Inside the Fight Against Revenge Porn," Time.com. The images may haunt victims throughout their lives.

This problem is widespread, with one recent study finding that "4% of U.S. internet users—roughly 10.4 million Americans—have been threatened with or experienced the posting of explicit images without their consent." See Data & Society, "New Report Shows That 4% of U.S. Internet Users Have Been a Victim of 'Revenge Porn,'" (Dec. 13, 2016); see also C. Alter, *supra* (stating that "Facebook received more than 51,000 reports of revenge porn in January 2017 alone"). Revenge porn is overwhelmingly targeted at women. D. Citron & M. Franks, *supra*, at 353–54.

II. Vermont's Statute

Vermont's law, enacted in 2015, makes it a crime punishable by not more than two years' imprisonment and a fine of $2,000 or both to "knowingly disclose a visual image of an identifiable person who is nude or who is engaged in sexual conduct, without his or her consent, with the intent to harm, harass, intimidate, threaten, or coerce the person depicted, and the disclosure would cause a reasonable person to suffer harm." 13 V.S.A. § 2606(b)(1). "Nude" and "sexual conduct" are both expressly defined. The law makes clear that "[c]onsent to recording of the visual image does not, by itself, constitute consent for disclosure of the image." Violation

of § 2606(b)(1) is a misdemeanor, unless a person acts "with the intent of disclosing the image for financial profit," in which case it is a felony.

Section 2606 does not apply to:

> (1) Images involving voluntary nudity or sexual conduct in public or commercial settings or in a place where a person does not have a reasonable expectation of privacy.
>
> (2) Disclosures made in the public interest, including the reporting of unlawful conduct, or lawful and common practices of law enforcement, criminal reporting, corrections, legal proceedings, or medical treatment.
>
> (3) Disclosures of materials that constitute a matter of public concern.
>
> (4) Interactive computer services, as defined in 47 U.S.C. § 230(f)(2), or information services or telecommunications services, as defined in 47 U.S.C. § 153, for content solely provided by another person. This subdivision shall not preclude other remedies available at law.

The law also provides a private right of action "against a defendant who knowingly discloses, without the plaintiff's consent, an identifiable visual image of the plaintiff while he or she is nude or engaged in sexual conduct and the disclosure causes the plaintiff harm."

III. Facts and Proceedings Before the Trial Court

In late 2015, defendant was charged by information with violating 13 V.S.A. § 2606(b)(1). In support of the charge, the State submitted an affidavit from a police officer . . . .

The police officer averred as follows. Complainant contacted police after she discovered that someone had posted naked pictures of her on a Facebook account belonging to Anthony Coon and "tagged" her in the picture. Complainant called Mr. Coon and left a message asking that the pictures be deleted. Shortly thereafter, defendant called complainant back on Mr. Coon's phone; she called complainant a "moraless pig" and told her that she was going to contact complainant's employer, a child-care facility. When complainant asked defendant to remove the pictures, defendant responded that she was going to ruin complainant and get revenge.

Complainant told police that she had taken naked pictures of herself and sent them to Mr. Coon through Facebook Messenger. She advised that the pictures had been sent privately so that no one else could view them. Defendant admitted to the officer that she saw complainant's pictures on Mr. Coon's Facebook account and that she posted them on Facebook using Mr. Coon's account. Defendant asked the officer if he thought complainant had "learned her lesson."

In her sworn statement, complainant provided additional details concerning the allegations above. She described her efforts to delete the pictures from Facebook and to delete her own Facebook account. Complainant stated that the night before the pictures were publicly posted, she learned through a friend that defendant was asking about her. Defendant described herself as Mr. Coon's girlfriend. Complainant asked Mr. Coon about defendant, and Mr. Coon said that defendant was obsessed with him and that he had never slept with her. Complainant "took it as him being honest so we moved on." The next day, complainant discovered that defendant posted her nude images on Mr. Coon's Facebook page.

At the court's request, defendant and the State later stipulated to the following additional facts for purposes of the motion to dismiss: complainant sent the photographs to Mr. Coon on October 7, 2015. The photographs were posted on a public Facebook page on October 8, 2015. Complainant was not in a relationship with Mr. Coon at the time the photographs were sent to him. Defendant did not have permission to access Mr. Coon's Facebook account. Mr.

Coon believed that defendant accessed his Facebook account through her telephone, which had Mr. Coon's password saved.

[T]he State argues that nonconsensual pornography, as defined in the Vermont statute, falls outside of the realm of constitutionally protected speech for two reasons: such speech amounts to obscenity, and it constitutes an extreme invasion of privacy unprotected by the First Amendment. Second, the State argues that even if nonconsensual pornography falls outside of the categorical exclusions to the First Amendment's protection of free speech, the statute is narrowly tailored to further a compelling State interest.

The Supreme Court has recognized that in a facial challenge to a regulation of speech based on overbreadth, a law may be invalidated if "a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." Defendant here does not frame her challenge to the statute as an overbreadth challenge but instead argues that insofar as the speech restricted by the statute is content-based, the statute is presumptively invalid and fails strict scrutiny review.

The protections of the First Amendment are not, however, absolute. The U.S. Supreme Court has "long recognized that the government may regulate certain categories of expression consistent with the Constitution." *Virginia v. Black* (2003). These well-defined and narrow categories of expression have "such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality."

For the reasons set forth below, we conclude that "revenge porn" does not fall within an established categorical exception to full First Amendment protection, and we decline to predict that the U.S. Supreme Court would recognize a new category. However, we conclude that the Vermont statute survives strict scrutiny as the U.S. Supreme Court has applied that standard.

A. Categorical Exclusions

1. Obscenity

Although some nonconsensual pornography may meet the constitutional definition of obscenity, we reject the State's contention that the Vermont statute categorically regulates obscenity and is thus permissible under the First Amendment.

The Supreme Court has recognized the government's "legitimate interest in prohibiting dissemination or exhibition of obscene material when the mode of dissemination carries with it a significant danger of offending the sensibilities of unwilling recipients or of exposure to juveniles." *Miller v. California* (1973). The Court has consistently recognized that a state's interest in regulating obscenity relates to protecting the sensibilities of those exposed to obscene works, as opposed to, for example, protecting the privacy or integrity of the models or actors depicted in obscene images.

By contrast, a state's interest in regulating nonconsensual pornography has little to do with the sensibilities of the people exposed to the offending images; the State interest in this case focuses on protecting the privacy, safety, and integrity of the victim subject to nonconsensual public dissemination of highly private images. In that sense, Vermont's statute is more analogous to the restrictions on child pornography that the Supreme Court has likewise categorically excluded from full First Amendment protection.

Given the ill fit between nonconsensual pornography and obscenity, and the Supreme Court's reluctance to expand the contours of the category of obscenity, we conclude that the speech restricted by Vermont's statute cannot be fairly categorized as constitutionally unprotected obscenity.

2. Extreme Invasion of Privacy

Although many of the State's arguments support the proposition that the speech at issue in this case does not enjoy full First Amendment protection, we decline to identify a new categorical exclusion from the full protections of the First Amendment when the Supreme Court has not yet addressed the question.

The Supreme Court recognized in *Stevens* that there may be "some categories of speech that have been historically unprotected, but have not yet been specifically identified or discussed as such in our case law." 559 U.S. at 472. In deciding whether to recognize a new category outside the First Amendment's full protections for depictions of animal cruelty, the Court focused particularly on the absence of any history of regulating such depictions, rather than the policy arguments for and against embracing the proposed new category.

The State makes a persuasive case that United States legal history supports the notion that states can regulate expression that invades individual privacy without running afoul of the First Amendment. It points to a host of statements by the Supreme Court over the years suggesting that the government may regulate speech about purely private matters that implicates privacy and reputational interests, an influential 1890 law review article by Samuel Warren and Louis Brandeis recognizing the right to privacy, and a well-established common law tort of publicity given to private life. The State's arguments in this regard are well-founded. (Court's review of *Cox Broadcasting*, *Florida Star*, and *Bartnicki* omitted.)

These U.S. Supreme Court decisions reflect three consistent themes: (1) speech on matters of private concern that implicate the privacy interests of nonpublic figures does not enjoy the same degree of First Amendment protection as speech on matters of public concern or relating to public figures; (2) state laws protecting individual privacy rights have long been established, and are not necessarily subordinate to the First Amendment's free speech protections; and (3) the Court is wary of broad rules or categorical holdings framing the relationship between laws protecting individual privacy and the First Amendment. (Court's discussion of Warren and Brandeis article omitted).

Notwithstanding these considerations, we decline to predict that the Supreme Court will add nonconsensual pornography to the list of speech categorically excluded. We base our declination on two primary considerations: the Court's recent emphatic rejection of attempts to name previously unrecognized categories, and the oft-repeated reluctance of the Supreme Court to adopt broad rules dealing with state regulations protecting individual privacy as they relate to free speech.

B. Strict Scrutiny

Our conclusion that nonconsensual pornography does not fall into an existing or new category of unprotected speech does not end the inquiry. The critical question is whether the First Amendment permits the regulation at issue. The remaining question is whether § 2606 is narrowly tailored to serve a compelling State interest.

1. Compelling Interest

We conclude that the State interest underlying § 2606 is compelling. We base this conclusion on the U.S. Supreme Court's recognition of the relatively low constitutional significance of speech relating to purely private matters, evidence of potentially severe harm to individuals arising from nonconsensual publication of intimate depictions of them, and a litany of analogous restrictions on speech that are generally viewed as uncontroversial and fully consistent with the First Amendment.

Although we decline to identify a new category of unprotected speech on the basis of the above cases, the decisions cited above are relevant to the compelling interest analysis in that they reinforce that the First Amendment limitations on the regulation of speech concerning

matters of public interest do not necessarily apply to regulation of speech concerning purely private matters. Time and again, the Supreme Court has recognized that speech concerning purely private matters does not carry as much weight in the strict scrutiny analysis as speech concerning matters of public concern, and may accordingly be subject to more expansive regulation.

The Court acknowledged that "the boundaries of the public concern test are not well defined," and offered the following guiding principles:

> Speech deals with matters of public concern when it can be fairly considered as relating to any matter of political, social, or other concern to the community, or when it is a subject of legitimate news interest; that is, a subject of general interest and of value and concern to the public. The arguably inappropriate or controversial character of a statement is irrelevant to the question whether it deals with a matter of public concern.

The proscribed speech in this case has no connection to matters of public concern. By definition, the proscribed images must depict nudity or sexual conduct; must be disseminated without the consent of the victim.; cannot include images in settings in which a person does not have a reasonable expectation of privacy; cannot include disclosures made in the public interest, including reporting concerning various specified matters; and may not constitute a matter of public concern. By definition, the speech subject to regulation under § 2606 involves the most private of matters, with the least possible relationship to matters of public concern.

Moreover, nonconsensual pornography is remarkably common, and the injuries it inflicts are substantial. A 2014 estimate set the number of websites featuring nonconsensual pornography at 3,000. *Revenge Porn: Misery Merchants*, THE ECONOMIST (July 5, 2014). That number has no doubt grown. One recent survey found that that two percent of U.S. internet users have been the victim of nonconsensual pornography—that is, someone actually posted an explicit video or image of them online without their consent. A. Lenhart, M. Ybarra, M. Price-Feeney, Data & Society Research Institute and Center for Innovative Public Health Research, *Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of "Revenge Porn,"* 4 (Dec. 13, 2016). A survey of victims of nonconsensual pornography found that in over fifty percent of the cases the nude images were published alongside the victim's full name and social network profile, and over twenty percent of victims reported that their email addresses and telephone numbers appeared alongside the images. D. Citron & M. Franks, *supra*, at 350–51.

The harm to the victims of nonconsensual pornography can be substantial. Images and videos can be directly disseminated to the victim's friends, family, and employers; posted and "tagged" (as in this case) so they are particularly visible to members of a victim's own community; and posted with identifying information such that they catapult to the top of the results of an online search of an individual's name. In the constellation of privacy interests, it is difficult to imagine something more private than images depicting an individual engaging in sexual conduct, or of a person's genitals, anus, or pubic area, that the person has not consented to sharing publicly. The personal consequences of such profound personal violation and humiliation generally include, at a minimum, extreme emotional distress. See *id*. at 351 (citing data that over eighty percent of victims report severe emotional distress and anxiety). Amici cited numerous instances in which the violation led the victim to suicide. Moreover, the posted images can lead employers to fire victims. A Microsoft-commissioned survey found that an internet search is a standard part of most employers' hiring processes. For that reason, nonconsensual pornography posted online can be a significant obstacle to getting a job. Moreover, the widespread dissemination of these images can lead to harassment, extortion, unwelcome sexual attention, and threats of violence. See D. Citron & M. Franks, *supra*, at 350–54. The government's interest in preventing any intrusions on individual privacy is substantial; it's at its highest when the invasion of privacy takes the form of nonconsensual pornography.

Finally, the government's interest in preventing the nonconsensual disclosure of nude or sexual images of a person obtained in the context of a confidential relationship is at least as strong as its interest in preventing the disclosure of information concerning that person's health or finances obtained in the context of a confidential relationship; content-based restrictions on speech to prevent these other disclosures are uncontroversial and widely accepted as consistent with the First Amendment. Doctors who disclose individually identifiable health information without permission may be subject to a $50,000 fine and a term of imprisonment for up to a year. 42 U.S.C. § 1320d-6. Banks are prohibited from disclosing to third-parties nonpublic, personal information about their customers without first giving the customers a chance to "opt out." 15 U.S.C. § 6802(b). In fact, in Vermont financial institutions can only make such disclosures if customers "opt in." And nonconsensual disclosure of individuals' social security numbers in violation of U.S. law can subject the discloser to fines and imprisonment for up to five years. 42 U.S.C. § 408(a)(8). In these cases, it is obvious that the harm to be addressed flows from the disclosure of personal information. The fact that the disclosure requires speech, and that restriction of that speech is based squarely on its content, does not undermine the government's compelling interest in preventing such disclosures. From a constitutional perspective, it is hard to see a distinction between laws prohibiting nonconsensual disclosure of personal information comprising images of nudity and sexual conduct and those prohibiting disclosure of other categories of nonpublic personal information. The government's interest in protecting all from disclosure is strong.

For the above reasons, we conclude that the State interest underlying § 2606 is compelling.

2. Narrowly Tailored

Section 2606 defines unlawful nonconsensual pornography narrowly, including limiting it to a confined class of content, a rigorous intent element that encompasses the nonconsent requirement, an objective requirement that the disclosure would cause a reasonable person harm, an express exclusion of images warranting greater constitutional protection, and a limitation to only those images that support the State's compelling interest because their disclosure would violate a reasonable expectation of privacy. Our conclusion on this point is bolstered by a narrowing interpretation of one provision that we offer to ensure that the statute is duly narrowly tailored. The fact that the statute provides for criminal as well as civil liability does not render it inadequately tailored.

The images subject to § 2606 are precisely defined, with little gray area or risk of sweeping in constitutionally protected speech.

Moreover, disclosure is only criminal if the discloser knowingly discloses the images without the victim's consent. § 2606(b)(1). We construe this intent requirement to require knowledge of both the fact of disclosing, and the fact of nonconsent. Individuals are highly unlikely to accidentally violate this statute while engaging in otherwise permitted speech. In fact, § 2606 goes further, requiring not only knowledge of the above elements, but a specific intent to harm, harass, intimidate, threaten, or coerce the person depicted or to profit financially.

In addition, the disclosure must be one that would cause a reasonable person "physical injury, financial injury, or serious emotional distress." § 2606(a)(2), (b)(1). The statute is not designed to protect overly fragile sensibilities, and does not reach even knowing, nonconsensual disclosures of images falling within the narrow statutory parameters unless disclosure would cause a reasonable person to suffer harm.

Two additional limitations assuage any concern that some content meeting all of these requirements may nonetheless implicate a matter of public concern. First, the statute does not purport to reach "[d]isclosures made in the public interest, including the reporting of unlawful conduct, or lawful and common practices of law enforcement, criminal reporting, corrections,

legal proceedings, or medical treatment." § 2606(d)(2). This broad and nonexclusive list of permitted disclosures is designed to exclude from the statute's reach disclosures that do implicate First Amendment concerns—those made in the public interest. Second, even if a disclosure is not made "in the public interest," if the materials disclosed "constitute a matter of public concern," they are excluded from the statute's reach. § 2606(d)(3).

We reject defendant's suggestion that civil penalties are necessarily less restrictive than criminal penalties, and that because the statute includes criminal penalties as well as the potential for civil liability it is broader than necessary to advance the State's interest. The Supreme Court has acknowledged that civil and criminal penalties do not stand in a clear hierarchy from the perspective of chilling speech. . . . In fact, the Court noted that people charged criminally enjoy greater procedural safeguards than those facing civil suit, and the prospect of steep civil damages can chill speech even more than that of criminal prosecution.

For the above reasons, the statute is narrowly tailored to advance the State's interests, does not penalize more speech than necessary to accomplish its aim, and does not risk chilling protected speech on matters of public concern. We accordingly conclude that 13 V.S.A. § 2606 is constitutional on its face.

SKOGLUND, J., dissenting.

First, I do not agree that the government has a compelling interest. . . . Can revenge porn cause extreme emotional distress? Oh, yes. However, while the majority finds a compelling state interest in preventing the nonconsensual disclosure of nude or sexual images of a person obtained in the context of a confidential relationship, I cannot agree that, in this day and age of the internet, the State can reasonably assume a role in protecting people from their own folly and trump First Amendment protections for speech.

Next, the statute fails to survive strict scrutiny because it is not narrowly tailored, nor does it provide the least restrictive means of dealing with the perceived problem. As explained above, the statute criminalizes dissemination of nude imagery or any sexual conduct of a person without that person's consent and with a bad motive. Reduced to its essential purpose, it criminalizes an invasion of personal privacy.

My primary war with the statute is simply this. The State has at its disposal less restrictive means to protect Vermonters against invasion of their privacy than subjecting a violator to a criminal penalty. Section 2606 does provide for a civil remedy. Subsection (e) provides plaintiff a private cause of action against a defendant who knowingly discloses, without the plaintiff's consent, an identifiable visual image of the plaintiff while he or she is nude or engaged in sexual conduct and the disclosure causes the plaintiff harm. It also provides for relief in the form of equitable relief, a temporary restraining order, a preliminary injunction or permanent injunction. While the State argued that the private right of action may fail to deter and punish publishers of nonconsensual pornography because "[m]ost victims lack resources to bring lawsuits, [and] many individual defendants are judgment-proof," the potential success of a private right of action is irrelevant in determining whether less restrictive alternative exists. One could always bring an action alleging intentional infliction of emotional distress. The Legislature could provide for triple damages and require that attorney's fees be awarded the prevailing party. There is a myriad of ways to provide protection to people short of criminal charges.

The statute's ambiguities concerning the scope of its coverage, even with the limiting interpretation crafted by the majority, coupled with its increased deterrent effect as a criminal statute, raise special First Amendment concerns because of its obvious chilling effect on free speech. "Criminal punishment by government, although universally recognized as a necessity in limited areas of conduct, is an exercise of one of government's most awesome and dangerous powers." *Ginzburg v. United States* (1966) (Black, J., dissenting). While disseminating "revenge porn" may be a repulsive and harmful action, the statute's attempt to criminalize this behavior

runs afoul of the rights and privileges of the First Amendment. When content-based speech regulation is in question, exacting scrutiny is required. And, the burden placed on free speech due to its content is unacceptable if less restrictive alternatives would be at least as effective in achieving the statute's purposes. Civil avenues exist that can avenge an invasion of privacy or a deliberate infliction of emotional distress without criminalizing speech based on the content of the message.

As Supplemented Following Further Briefing

ROBINSON, J.

We conclude that dismissal is appropriate because the State has not established that it has evidence showing that complainant had a reasonable expectation of privacy in the images she sent to Mr. Coon. . . . Because the State has stipulated that complainant and Mr. Coon were not in a relationship at the time complainant sent Mr. Coon the photo, and there is no evidence in the record showing they had any kind of relationship engendering a reasonable expectation of privacy, we conclude the State has not met its burden.

The requirement that the images at issue be subject to a reasonable expectation of privacy is central to the statute's constitutional validity under a strict-scrutiny standard. A content-based restriction on First Amendment-protected speech like § 2606 can withstand strict scrutiny only if it is narrowly tailored to serve a compelling state interest. The compelling state interest underlying § 2606 is "to protect peoples' reasonable expectations of privacy in intimate images of them," and prevent the serious harms that can result when those expectations are broken. We noted that "[w]here an individual does not have a reasonable expectation of privacy in an image, the State's interest in protecting the individual's privacy interest in that image is minimal." Where the State has only a minimal interest at stake—such as where the individual depicted did not have a reasonable expectation of privacy—a prosecution under § 2606 would not be a justifiable incursion upon First Amendment-protected speech. Our conclusion that § 2606 is narrowly tailored insofar as it penalizes only the disclosure of images in which the depicted person had a reasonable expectation of privacy rested in part on our construction that the statute would apply only where the person depicted had not distributed the images in a way that would undermine their reasonable expectation of privacy.

The State has not shown it has evidence that complainant had a reasonable expectation of privacy in the images she sent to Mr. Coon. We understand this to be an objective standard, and find no evidence in the record showing that complainant had such a relationship with Mr. Coon that distributing the photos to him did not undermine any reasonable expectation of privacy that she had in them.

We do not attempt to precisely define here where and when a person may have a reasonable expectation of privacy for the purposes of § 2606(d)(1), except to note that it generally connotes a reasonable expectation of privacy within a person's most intimate spheres. Privacy here clearly does not mean the exclusion of all others, but it does mean the exclusion of everyone but a trusted other or few.

Notes

1. *Civil or criminal?* The Vermont statute allowed for both civil and criminal penalties. Some other states allow for only one or the other. Why might criminal sanctions be preferrable here? Some advocates have argued that fear of criminal prosecution is uniquely able to deter potential offenders, and that the high costs of a cyber investigation are most easily borne by the government.
2. Is the government simply protecting people from their own folly? Justice Marilyn Skoglund certainly thought so. What types of speech are facilitated by having a law on nonconsensual pornography? What types are inhibited by it? Can people reasonably protect themselves from harm absent laws like Vermont's?

3. What sort of prior interaction is necessary to establish an expectation of privacy? Is mutual flirtation enough? Does there need to be some explicit comment about confidentiality? This sounds like an issue of community norms, but that raises the question of how such norms can be assessed and which community's norms are important in a given circumstance. Here, the Court leaned heavily on a stipulation that the claimant and Mr. Coon were not in a "relationship." In its briefing to the Court, the state tried to argue around this stipulation, pointing out, first, that the communications between Coon and the claimant suggest some connection (especially as Coons is telling the claimant that he is not sleeping with another woman) and, second, that the meaning of "relationship" is actually quite vague and uncertain. Though the Court was not persuaded, this may be a case where an early-litigation stipulation sank an otherwise winnable prosecution.
4. There is variation in how states have written their nonconsensual-pornography statutes. Most notably, some states have omitted the "intent to harm" requirement seen in Vermont law, while others have included it. Think through the social realities of nonconsensual pornography distribution. Though harm may often result from distribution, that harm may be incidental to the distributor's goals. Surveys of nonconsensual pornography offenders have shown that much distribution is done for purposes of bragging.[47] This would not fall within the Vermont criminal statute, which requires "the intent to harm, harass, intimidate, threaten, or coerce the person depicted." It would fall within the Vermont civil statute, however, which omits that requirement entirely.
5. Why are these images so harmful? In a way, a nude image conveys very little information. Humans generally have skin under their clothes. Given a clothed picture of a person, both humans and computer programs can guess at the approximate appearance of that skin.[48] So the informational harm of a nude image is relatively slight. Yet there is broad agreement that there is a strong dignitary violation, and there are real consequences to the distribution of these images. What do we make of that? Why would a childcare facility, for instance, have a negative reaction to one of its employees being a victim of nonconsensual pornography?
6. Speaking of that broad agreement, nonconsensual-pornography laws have proliferated with shocking speed.[49] Nearly every state now has such a law (48 as of 2024), while no state had such a law in 2010. Why might this be?
7. *Katie Hill.* In 2019, then-Representative Katie Hill of California was accused of having an inappropriate sexual relationship with one of her male congressional aides (which would have violated House rules) and of having previously had a polyamorous relationship with her husband and a female campaign staffer (which did not violate any explicit rules). The *RedState* article setting out the accusations included nude photos of Hill with the campaign staffer. The photos used black bars to censor nipples and genitals. According to Hill, the photos were leaked by her husband, whom she also claimed was abusive. After resigning, Hill sued *RedState* and other media organizations, but lost on the grounds that the photos were a matter of public concern. One of the story's authors defended the piece by saying, "The story is not about anything other than Hill's behavior as a candidate and congresswoman, and her use of power for sexual satisfaction." Hill was then ordered to pay attorneys' fees for several of the defendants, amounting to $220,000, under anti SLAAP laws.

---

[47] See, e.g., Asia A. Eaton and Clare McGlynn, *The Psychology of Nonconsensual Porn: Understanding and Addressing a Growing Form of Sexual Violence*, 7 POLICY INSIGHTS FROM THE BEHAVIORAL AND BRAIN SCIENCES 190 (2020); Nicola Henry and Asher Flynn, *Image-based sexual abuse. Online distribution channels and illicit communities of support,* 25 VIOLENCE AGAINST WOMEN 1932 (2019).

[48] One of the less savory uses of generative AI is to undress clothed images of people.

[49] *See generally* Mary Anne Franks, *"Revenge Porn" Reform: A View from the Front Lines*, 69 FLA. L. REV. 1251 (2017) (reviewing the rapid expansion of nonconsensual-pornography laws from 2013 to 2017)

Federal law first incorporated a civil cause of action for nonconsensual dissemination of pornographic images in 2022. 15 U.S.C. § 6851.

15 U.S. Code § 6851 - Civil action relating to disclosure of intimate images

In 2022, the federal government created a national civil cause of action for nonconsensual pornography.

(a) Definitions

(2) Consent. The term "consent" means an affirmative, conscious, and voluntary authorization made by the individual free from force, fraud, misrepresentation, or coercion.

(3) Depicted individual. The term "depicted individual" means an individual whose body appears in whole or in part in an intimate visual depiction and who is identifiable by virtue of the person's face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature, or from information displayed in connection with the visual depiction.

(5) Intimate visual depiction. The term "intimate visual depiction"—

(A) means a visual depiction . . . that depicts—

(i) the uncovered genitals, pubic area, anus, or post-pubescent female nipple of an identifiable individual; or

(ii) the display or transfer of bodily sexual fluids—

(I) on to any part of the body of an identifiable individual;

(II) from the body of an identifiable individual; or

(III) an identifiable individual engaging in sexually explicit conduct and

(B) includes any visual depictions described in subparagraph (A) produced while the identifiable individual was in a public place only if the individual did not—

(i) voluntarily display the content depicted; or

(ii) consent to the sexual conduct depicted.

(b) Civil action

(1) Right of action. [A]n individual whose intimate visual depiction is disclosed, in or affecting interstate or foreign commerce or using any means or facility of interstate or foreign commerce, without the consent of the individual, where such disclosure was made by a person who knows that, or recklessly disregards whether, the individual has not consented to such disclosure, may bring a civil action against that person in an appropriate district court of the United States . . . .

(2) Consent

(A) the fact that the individual consented to the creation of the depiction shall not establish that the person consented to its distribution; and

(B) the fact that the individual disclosed the intimate visual depiction to someone else shall not establish that the person consented to the further disclosure of the intimate visual depiction by the person alleged to have violated paragraph (1).

(3) Relief. (i) [A]n individual may recover the actual damages sustained by the individual or liquidated damages in the amount of $150,000, and the cost of the action, including reasonable attorney's fees and other litigation costs reasonably incurred; and (ii) the court may . . . order equitable relief . . . .

(4) Exceptions. An identifiable individual may not bring an action for relief under this section relating to—

(A) an intimate image that is commercial pornographic content . . .
(B) a disclosure made in good faith—
(i) to a law enforcement officer or agency;
(ii) as part of a legal proceeding;
(iii) as part of medical education, diagnosis, or treatment; or
(iv) in the reporting or investigation of—
(I) unlawful content; or
(II) unsolicited or unwelcome conduct;
(C) a matter of public concern or public interest; or
(D) a disclosure reasonably intended to assist the identifiable individual.

Notes

1. Note that the federal cause of action lacks an intent to harm requirement, initially lacked a criminal provision, and contains massive statutory damages. It keeps the "matter of public concern" exception, along with a variety of others.
2. Think about how some of the exceptions might come into play. For example, 4(D) involves a disclosure reasonably intended to assist the individual. Once I sought to help a friend get a pornographic image taken down from a social networking site. To do this, I needed to send a link to the image to a friend with contacts at the site.

One emerging issue in nonconsensual pornography is deepfake pornography. Deepfakes are videos that use machine-learning algorithms to digitally impose one person's face and voice onto videos of other people.[50] The resulting doctored videos show people doing and saying things they never did or said. According to one estimate, ninety-six percent of all deepfake videos are pornographic, and those depicted in pornographic deepfakes are almost exclusively women.[51] Nonpornographic deepfake videos have depicted politicians, corporate figures, and celebrities.

The scholarly literature on deepfakes identifies two types of harm: dignitary harms to the individuals depicted in the videos (whether viewers believe the videos are real or not) and reputational, political, and national security harms to society from successfully deceptive videos. Yet there are few legal protections for individuals depicted in deepfakes under traditional privacy law, and what law does exist—for example, defamation law—tends to address only deception-related harms and not dignitary violations. The general problem is that the major privacy torts target those who obtain or publicize information that is both true and private. These torts are a poor match for the typical case of pornographic deepfakes, where that which is true (the person's face) is not private, and that which is private (the sex act) is not true.

Even traditional nonconsensual-pornography laws fail to address deepfake pornography. Statutory language often defines the depicted individual as the one whose genitals, nipples, etc. are being shown. In deepfakes, they are not. Also, the statutes generally require that images be created or obtained with an expectation of privacy or confidentiality, which deepfakes are not.

In 2019, California passed two measures: one creating a civil cause of action for those featured in pornographic deepfakes and the other prohibiting the dissemination of unlabeled,

---

[50] Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1758 (2019).

[51] HENRY AJDER, GIORGIO PATRINI, FRANCESCO CAVALLI & LAURENCE CULLEN, DEEPTRACE, THE STATE OF DEEPFAKES: LANDSCAPE, THREATS, AND IMPACT (2019). Although one study found that 100% of pornographic deepfake videos targeted women, there are some pornographic deepfake videos of male celebrities.

altered videos containing political candidates in the two months leading up to an election.[52] Similarly, Virginia expanded its nonconsensual-pornography statute to cover morphed videos,[53] and Texas protected candidates in the lead-up to elections.[54] New York has passed new legislation expanding its nonconsensual-pornography law and providing limited protection against commercial uses of deepfakes.[55] As nonconsensual-pornography laws proliferated greatly over the 2010s, deepfake laws seem poised to expand in the 2020s.

Deepfake pornography forces courts and legislatures to consider why nonconsensual pornography is wrong. If the primary harm from nonconsensual pornography is either informational or related to a breach of trust in the leaking of the images, then deepfake pornography is completely different: deepfakes can be produced without violating trust and without revealing nonpublic information. But if the problem with nonconsensual pornography instead stems from involuntary sexualization or misappropriation of sexual identity, then deepfakes are creating the equivalent harm.

A series of survey studies that I conducted with Carly Pace in 2020 and 2021 showed that many people believe deepfakes are wrong.[56] First, participants viewed deepfake videos as more wrongful and harmful than written accounts describing the same conduct, meaning there was extra harm from the change to a video medium. Second, ninety-two percent of participants wanted to criminalize the dissemination of a pornographic deepfake even if it was clearly labeled as fake. Pornographic deepfakes featuring celebrities (as opposed to everyday people) and non-nude but sexualized conduct were also nearly universally condemned. These reactions do not merely reflect common opposition to pornography in all its forms: prior research has shown that significantly fewer people—only about thirty percent of the public—want to criminalize pornography more generally.[57] A smaller follow-up study showed that participants generally support allowing for both civil and criminal causes of action against those who produce deepfakes. Finally, a second follow-up study showed that people judge the dissemination of pornographic deepfakes as equally as harmful as the dissemination of traditional nonconsensual pornography. They also consider deepfake pornography marginally more morally blameworthy.

In contrast, participants considered nonpornographic deepfakes substantially less wrongful if they did not depict inherently defamatory conduct, such as illegal drug use, or if they were clearly labeled as fake. However, many participants still wished to assign criminal liability even for the creation of less obviously harmful nonpornographic deepfake videos, such as one depicting a deceased scientist describing their life's work.

Bans on deepfake videos will likely be subject to First Amendment challenges. Under existing precedent, mere falsity of a message is not enough to justify a ban. In *United States v. Alvarez*, the Supreme Court struck down the Stolen Valor Act, which made it a crime to make false statements about receiving military decorations or medals.[58] The Court reasoned that it

---

[52] CAL. CIV. CODE § 1708.86 (West 2020) (creating a civil cause of action for those nonconsensually depicted in altered videos that show them engaging in sexually explicit conduct); CAL. ELEC. CODE § 20010 (West 2023) (prohibiting unlabeled, altered videos featuring political candidates in the two months prior to an election).

[53] VA. CODE ANN. § 18.2-386.2 (West 2024).

[54] TEX. ELEC. CODE ANN. § 255.004(d) (West 2019). This was held unconstitutional be an intermediate Texas appellate court in 2023 and is pending further proceedings. *Ex parte Stafford*, 667 S.W.3d 517 (Tex. App. 2023), petition for discretionary review granted (Aug. 23, 2023).

[55] N.Y. CIV. RIGHTS LAW §§ 50-F, 52-C (McKinney 2021).

[56] Matthew B. Kugler & Carly Pace, *Deepfake Privacy: Attitudes and Regulation*, 116 NW. U. L. REV. 611 (2021).

[57] Charles Fain Lehman, *What Do Americans Think About Banning Porn?*, INST. FOR FAM. STUD. (Dec. 18, 2019), https://ifstudies.org/blog/what-do-americans-think-about-banning-porn.

[58] *United States v. Alvarez*, 567 U.S. 709, 715 (2012).

had never held that falsity alone was outside First Amendment protection.[59] Rather, false statements fall outside First Amendment protection when there are additional considerations, such as "some other legally cognizable harm associated with [the] false statement"[60] or "[w]here false claims are made to effect a fraud or secure moneys or other valuable considerations, say, offers of employment."[61]

Nevertheless, there are substantial similarities between the privacy harms of deepfake pornography and the harms of nonconsensual pornography—and bans on nonconsensual pornography have generally been upheld. As with nonconsensual pornography, victims of deepfake pornography report various harms, including harassment and threats.[62] The above-described survey responses are also consistent with the notion that deepfake pornography, both labeled and unlabeled, is extremely harmful and an affront to the dignity of the person depicted. Nonconsensual pornography and deepfake pornography both involve a type of dignitary harm that stems from one's ability to control information about oneself. Traditional nonconsensual pornography involves disclosure of personal information, which "can severely inhibit a person's autonomy and self-development."[63] Deepfake pornography creates similar harm as a "distortion" that manipulates "the way a person is perceived and judged by others, and involves the victim being inaccurately exposed to the public."[64] Much like the painful accuracy of nonconsensually disclosed pornography, the misrepresentation of deepfake pornography impacts one's ability to control their sexual identity.

In a parallel context, federal appellate courts have consistently held that morphed images and videos depicting child pornography—those that superimpose the face of a child on a nude or sexualized body—still qualify as child pornography and can be constitutionally prosecuted as such. In agreeing with the Second and Sixth Circuits that morphed child pornography is not protected speech, the Fifth Circuit noted, "By using identifiable images of real children, these courts conclude, morphed child pornography implicates the reputational and emotional harm to children that has long been a justification for excluding real child pornography from the First Amendment."[65] In effect, fake child pornography that appears to feature a real child can be criminalized for a subset of the same reasons that real child pornography featuring that child can be criminalized.

Incidentally, this line of case law has been largely overlooked in discussions of deepfake pornography of high schoolers. A person making a deepfake pornographic video of a 16-year-old may not be prosecutable or civilly liable under the state's nonconsensual-pornography statute but is very likely in violation of federal and state child-pornography law, which is notoriously extreme in its punishments.

---

[59] *Id*. at 719 ("The Court has never endorsed the categorical rule the Government advances: that false statements receive no First Amendment protection. . . . Even when considering some instances of defamation and fraud, moreover, the Court has been careful to instruct that falsity alone may not suffice to bring the speech outside the First Amendment. The statement must be a knowing or reckless falsehood.").

[60] *Id*.

[61] *Id*. at 723.

[62] *See, e.g.*, Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1886, 1921–23 (2019) (describing a female journalist targeted on social media with attitudinal and pornographic deepfake videos); Drew Harwell, *Fake-Porn Videos Are Being Weaponized to Harass and Humiliate Women: 'Everybody Is a Potential Target,'* WASH. POST (Dec. 30, 2018), https://www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-being-weaponized-harass-humiliate-women-everybody-is-potential-target/ (describing pornographic deepfake videos as being "weaponized disproportionately against women, representing a new and degrading means of humiliation, harassment, and abuse").

[63] Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 Duke L.J. 967, 991 (2003).

[64] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 547 (2006).

[65] United States v. Mecham, 950 F.3d 257, 265 (5th Cir. 2020).

The merits of First Amendment challenges to non-pornographic deepfakes present harder questions. Laws such as the election proximity laws would need to be evaluated based on how well they are tailored to their particular purposes. Already we have seen some First Amendment challenges there.[66] It is likely that courts will need considerable time before they reach stable and consistent judgments here as our understandings of deepfakes and their harms will likely evolve substantially during the 2020s.

The Take It Down Act

2025 saw the passage of a federal criminal nonconsensual pornography and nonconsensual pornographic deepfake law, the Take It Down Act.[67] It passed both the House and Senate with near-unanimous support. The Act imposes harsh prison sentences on individuals who knowingly publish or threaten to publish nonconsensual pornography, including AI-generated deepfakes. Specifically, it is unlawful to publish a nonconsensual intimate image (defined as in the federal civil provision above) of an *identifiable* person, if:

> (i) the intimate visual depiction was obtained or created under circumstances in which the person knew or reasonably should have known the identifiable individual had a reasonable expectation of privacy;
>
> (ii) what is depicted was not voluntarily exposed by the identifiable individual in a public or commercial setting;
>
> (iii) what is depicted is not a matter of public concern; and
>
> (iv) publication of the intimate visual depiction—
>
> > (I) is intended to cause harm; or
> >
> > (II) causes harm, including psychological, financial, or reputational harm, to the identifiable individual.

There are further exceptions for reporting such images to law enforcement or making disclosures reasonably calculated to aid victims. The provisions for deepfakes portion are similar, requiring the "digital forgery" be published without the consent of the identifiable individual, not be a matter of public concern, and be intended to cause harm. Digital forgeries are defined as computer created or modified intimate images (as defined in § 6851) "that, when viewed as a whole by a reasonable person, is indistinguishable from an authentic visual depiction of the individual." Broadly speaking, these provisions are in line with many state laws.

The novel portion of the act concerned the requirement that online platforms implement a process through which individuals can report intimate depictions and request their removal. Upon receiving valid notice, platforms must remove the content and any identical copies within 48 hours. The bill further provides a liability shield for platforms that over remove claimed nonconsensual pornography in good faith. Noncompliance with these takedown requirements would be treated as an unfair or deceptive act under the jurisdiction of the Federal Trade Commission.

The Take It Down Act has drawn criticism from various corners. Some argue that, unlike the DMCA on which it is modeled, the Act lacks essential safeguards—such as penalties for

---

[66] See, e.g., Kohls v. Bonta, No. 2:24-CV-02527 JAM-CKD, 2024 WL 4374134, at *8 (E.D. Cal. Oct. 2, 2024) (describing the CA election proximity law as a "hammer instead of a scalpel, serving as a blunt tool that hinders humorous expression and unconstitutionally stifles the free and unfettered exchange of ideas which is so vital to American democratic debate" and temporarily enjoining its enforcement.)

[67] S. 146, 119th Cong. (2025), available at https://www.congress.gov/bill/119th-congress/senate-bill/146 (last visited May 19, 2025).

malicious takedown requests or a counter-notice mechanism—raising concerns that platforms, overwhelmed by reports, will default to over-removal.[68] Unlike the narrowly tailored criminal provisions, the takedown requirements are broadly defined and do not require close scrutiny of consent or a reasonable expectation of privacy. As a result, legitimate content—such as journalistic photos of topless protests, law enforcement images of public offenders, or consensually shared adult material falsely flagged as nonconsensual—could be unjustly removed. Critics also warn that the Act could be misused by public figures involved in sexual scandals, with Donald Trump himself stating he would take advantage of it.[69] Others caution that the Act may burden encrypted service providers, potentially forcing them to abandon encryption, thereby jeopardizing internet privacy.[70]

Notes

1. The Take it Down Act has already been used in several federal criminal cases. In one, the defendant allegedly harassed multiple female victims using threatened dissemination of AI-generated photos to coerce the victims to share real ones. He also produced sexual images of minors.[71] In two others, the offenders allegedly posted AI-generated images of public figures (celebrities) and non-public figures (friends and classmates from high school) on a pornographic website.[72] In two of the three cases, the defendants used various tools to attempt to hide their identities but, obviously, they were not entirely successful.

---

[68] Cyber Civil Rights Initiative, CCRI Statement on the Passage of the TAKE IT DOWN Act (S. 146) (Apr. 28, 2025), https://cybercivilrights.org/ccri-statement-on-the-passage-of-the-take-it-down-act-s-146/.

[69] David Inserra, TAKE IT DOWN Act Shows That Noble Intentions Can Make Bad Tech Policy, Cato Inst.: Cato at Liberty Blog (Apr. 16, 2025), https://www.cato.org/blog/take-it-down-act-shows-noble-intentions-can-make-bad-tech-policy.

[70] Joe Mullin, The TAKE IT DOWN Act: A Flawed Attempt to Protect Victims That Will Lead to Censorship, Electronic Frontier Foundation Deeplinks Blog (Feb. 11, 2025), https://www.eff.org/deeplinks/2025/02/take-it-down-act-flawed-attempt-protect-victims-will-lead-censorship.

[71] USA v. Strahler, Docket No. 2:25-mj-00377 (S.D. Ohio June 23, 2025). The defendant pled guilty to cyberstalking, producing obscene visual representations of child sexual abuse and publication of digital forgeries. See Bonnie Eslinger, *Ohio Man First To Be Convicted Under Anti-Revenge Porn Law* Law360 (April 9, 2026). https://www.law360.com/articles/2463664/ohio-man-first-to-be-convicted-under-anti-revenge-porn-law

[72] USA v. Shannon, Docket No. 1:26-mj-00096 (E.D.N.Y. May 15, 2026). USA v. Hernandez, Docket No. 1:26-mj-00097 (E.D.N.Y. May 15, 2026). See Parker Quinlan, *Feds Announce First 'Deepfake' Law Arrests In Brooklyn*, Law360 (May 20, 2026).

III. Government Investigations

A. Fourth Amendment and law enforcement searches 135
1) The *Katz* Test 136
Katz v. United States, 389 U.S. 347 (1967) 137
United States v. White, 401 U.S. 745 (1971) 140
2) The Third-Party Doctrine 143
Smith v. Maryland, 442 U.S. 735 (1979) 143

B. Constitutional limitations and new technologies 148
1) Changing surveillance and communication technologies 149
Kyllo v. United States, 533 U.S. 27 (2001) 149
United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) 152
2) Location Tracking 156
United States v. Jones, 565 U.S. 400 (2012) 156
Carpenter v. United States, 585 U.S. 296 (2018) 163
Chatrie v. United States, 609 U.S. ___ (2026) 172
3) Digital Searches 185
Riley v. California, 573 U.S. 373 (2014) 186

C. Constitutional limitations on non-law enforcement searches 193
Vernonia School Dist. 47J v. Acton, 515 U.S. 646 (1995) 194
Ferguson v. City of Charleston, 532 U.S. 67 (2001) 200

D. Wiretapping and the Electronic Communications Privacy Act 206
1) The Wiretap Act 207
a) Interception by the government 209
b) Interception by private actors and penalties 210
c) Exclusionary rule 210
2) State Wiretap Law 211
3) The Pen Register Act 212
4) The Stored Communications Act 213
a) Required disclosures under 18 U.S.C § 2703 214
b) Limits on voluntary disclosure under 18 U.S.C § 2702 215
c) Penalties 215

The government gathers information for many purposes. It regulates everything from building codes, to speed limits, to lawn maintenance, to homicide. When most people think about privacy and government investigations, however, they tend to think of criminal investigations. And this is indeed where the largest body of case law has grown. There are many reasons for this. Likely first among them is the interaction between the very large volume of criminal defendants and the exclusionary rule, which sometimes requires the suppression of improperly obtained evidence. It is not uncommon for a criminal case to turn entirely on whether obvious evidence of guilt—be it a kilogram of cocaine or a gigabyte of child sex abuse material—can be properly entered into evidence.

This chapter begins with that common case, considering when the government's collection of information for law enforcement purposes violates constitutional protections. The aim in this section is not to convey a comprehensive knowledge of search-and-seizure law.[73]

[73] Your school likely offers a class in criminal procedure. We must leave something for that professor to teach you.

Instead it seeks to use the extensively litigated topics here to help answer a general question: What is private, and from whom?

A. Fourth Amendment and law enforcement searches

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Since the protection is against "unreasonable" "searches" and "seizures," one first asks whether an act of government information collection constitutes a "search" and then, second, whether the search is a reasonable one. The main theme of this section is the examination of what constitutes a search. As you will see, this has changed over time and remains highly debatable. Government information-gathering that does not rise to the level of a "search" is generally outside of Fourth Amendment regulation.

If something is a search, one then examines the reasonableness of that search. In the criminal investigation context, a "search" is reasonable if either a warrant is obtained or an exception to the warrant requirement applies. This is a binary choice: either a warrant is required, or it is not. There is no half-warrant or super-warrant in constitutional terms for standard law enforcement searches.[74] In other contexts, the rules are different (see in particular Chapter III.C on non-law enforcement searches).

To obtain a search warrant, the law enforcement officer must demonstrate probable cause that a search will turn up admissible evidence. The warrant application must explain the basis of this probable cause, state with particularity what will be searched, and describe what is expected to be found. A court authority, usually a magistrate, will consider the totality of circumstances to determine whether to issue the warrant.

Imagine a previously reliable informant has told a police officer that a particular person has illegal drugs stored in their bedroom. The officer could then apply for a warrant to search the person's bedroom for drugs and associated evidence. If granted, this warrant would give the officers the right to enter the person's home—otherwise impermissible under the Fourth Amendment—and to search that particular bedroom for drugs and associated evidence. This warrant would not grant officers the right to search the suspect's garage, however. Since the reliable informant only provided evidence of illegal drugs in the person's bedroom, the officers do not have probable cause to believe that such a search would yield admissible evidence.

There are a multitude of exceptions to the warrant requirement. The most common exception is consent. It is a search for the government to enter your home. With the permission of a resident, however, the government is free to enter. Anything the government observes while it is lawfully in your house can then be used as evidence. The consent exception plays a huge role in actual police practice. People often grant consent to searches even though those searches will ultimately lead to their arrest.

The government can also conduct a warrantless search of a person incident to that person's lawful arrest. There are many reasons for this exception—explored in the *Riley* excerpt

---

[74] Statutes can and do create vehicles for obtaining evidence that either require more or less process than traditional warrants. But these layer on top of constitutional requirements.

below. In short, however, the overarching rationale for the search-incident-to-arrest exception is that the government needs to know what is in the immediate possession of a person who is being taken into custody.

The government can also conduct a warrantless search under exigent circumstances. This exception requires the officer to have probable cause that a crime was being or had been committed; believe the circumstances were such that a reasonable person would think that the officer's search was necessary to prevent the destruction of evidence or similar; and have insufficient time to get a warrant.

There are also a variety of other warrant exceptions. A community caretaking exception (think a privacy intrusion while police officer is helping an elderly community member after a slip and fall), an automobile exception (think of this as an extension of exigency), and border searches.[75]

Evidence obtained from a search that was not supported by a warrant or authorized by an exception to the warrant requirement can be suppressed under the exclusionary rule. Thus, there are many cases litigating 1) whether a warrant was required and 2) whether a warrant exception applied. The purpose of the exclusionary rule is to disincentivize police misconduct. It is believed that law enforcement officials will be less inclined to conduct illegal searches if they cannot later use the evidence so obtained at trial.

Finally, it is important to understand the role of the good-faith exception in Fourth Amendment practice. If government officials acted in the good-faith belief that their search was lawful, the evidence will be admissible even if the search is later found to be illegal. Evidence should only be suppressed "if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *United States v. Leon*, 468 U.S. 897, 919 (1984). So, when the police act in *reasonable* reliance on a warrant that was defective in some respect, the evidence will still be admissible. More importantly, however, evidence obtained *prior to a change in law* will be admissible. So, imagine a police officer, in reasonable reliance on existing precedent, conducts a search of a suspect's computer. A court later extends the scope of Fourth Amendment protection to hold that this search violates the Fourth Amendment. If the officer was reasonable in their reliance on prior case law in thinking that the search was constitutionally reasonable, the evidence will be admitted anyway.

1) The *Katz* Test

In 1928, the Supreme Court held in *Olmstead v. United States*, 277 U.S. 438, 466 (1928) that the installation of a wiretap was not a Fourth Amendment violation absent a trespass on the suspect's property. By contrast, when a trespass did occur, even a comparatively trivial one, it was a Fourth Amendment violation. This understanding was substantially revised in *Katz v. United States*, which set the terms of the Fourth Amendment discourse for the subsequent fifty years.

---

[75] Because of the awkward interaction between low expectations of privacy at the border and high privacy interests in the contents of electronic devices, the subject of computer searches at the border has been examined in innumerable student notes, including my own. Matthew B. Kugler, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study,* 81 U. CHI. L. REV. 1165 (2014).

Katz v. United States, 389 U.S. 347 (1967)

JUSTICE STEWART delivered the opinion of the Court.

The petitioner was convicted in the District Court for the Southern District of California under an eight-count indictment charging him with transmitting wagering information by telephone from Los Angeles to Miami and Boston in violation of a federal statute. At trial the Government was permitted, over the petitioner's objection, to introduce evidence of the petitioner's end of telephone conversation, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls. We granted certiorari in order to consider the constitutional questions thus presented.

The petitioner had phrased those questions as follows:

> 'A. Whether a public telephone booth is a constitutionally protected area so that evidence obtained by attaching an electronic listening recording device to the top of such a booth is obtained in violation of the right to privacy of the user of the booth.
>
> B. Whether physical penetration of a constitutionally protected area is necessary before a search and seizure can be said to be violative of the Fourth Amendment to the United States Constitution.'

We decline to adopt this formulation of the issues. In the first place the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.' Secondly, the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the protection of a person's general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States.

Because of the misleading way the issues have been formulated, the parties have attached great significance to the characterization of the telephone booth from which the petitioner placed his calls. The petitioner has strenuously argued that the booth was a 'constitutionally protected area.' The Government has maintained with equal vigor that it was not. But this effort to decide whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected' deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside. But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

The Government contends, however, that the activities of its agents in this case should not be tested by Fourth Amendment requirements, for the surveillance technique they employed involved no physical penetration of the telephone booth from which the petitioner placed his calls. It is true that the absence of such penetration was at one time thought to foreclose further Fourth Amendment inquiry, for that Amendment was thought to limit only searches and seizures of tangible property. But '(t)he premise that property interests control the right of the Government to search and seize has been discredited.' Thus, although a closely divided Court supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested. Indeed, we have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements overheard without any 'technical trespass under local property law.'

We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.

The question remaining for decision, then, is whether the search and seizure conducted in this case complied with constitutional standards. In that regard, the Government's position is that its agents acted in an entirely defensible manner: They did not begin their electronic surveillance until investigation of the petitioner's activities had established a strong probability that he was using the telephone in question to transmit gambling information to persons in other States, in violation of federal law. Moreover, the surveillance was limited, both in scope and in duration, to the specific purpose of establishing the contents of the petitioner's unlawful telephonic communications. The agents confined their surveillance to the brief periods during which he used the telephone booth,[14] and they took great care to overhear only the conversations of the petitioner himself.[15]

Accepting this account of the Government's actions as accurate, it is clear that this surveillance was so narrowly circumscribed that a duly authorized magistrate, properly notified of the need for such investigation, specifically informed of the basis on which it was to proceed, and clearly apprised of the precise intrusion it would entail, could constitutionally have authorized, with appropriate safeguards, the very limited search and seizure that the Government asserts in fact took place.

The Government urges that, because its agents relied upon the decisions in *Olmstead* and *Goldman*, and because they did no more here than they might properly have done with prior judicial sanction, we should retroactively validate their conduct. That we cannot do. It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for

---

[14] Based upon their previous visual observations of the petitioner, the agents correctly predicted that he would use the telephone booth for several minutes at approximately the same time each morning. The petitioner was subjected to electronic surveillance only during this predetermined period. Six recordings, averaging some three minutes each, were obtained and admitted in evidence. They preserved the petitioner's end of conversations concerning the placing of bets and the receipt of wagering information.

[15] On the single occasion when the statements of another person were inadvertently intercepted, the agents refrained from listening to them.

detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order.

The Government does not question these basic principles. Rather, it urges the creation of a new exception to cover this case. It argues that surveillance of a telephone booth should be exempted from the usual requirement of advance authorization by a magistrate upon a showing of probable cause. We cannot agree. Omission of such authorization 'bypasses the safeguards provided by an objective predetermination of probable cause, and substitutes instead the far less reliable procedure of an after-the-event justification for the search, too likely to be subtly influenced by the familiar shortcomings of hindsight judgment.' And bypassing a neutral predetermination of the scope of a search leaves individuals secure from Fourth Amendment violations 'only in the discretion of the police.'

These considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. The government agents here ignored 'the procedure of antecedent justification that is central to the Fourth Amendment,' a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case. Because the surveillance here failed to meet that condition, and because it led to the petitioner's conviction, the judgment must be reversed.

Justice HARLAN, concurring.

As the Court's opinion states, 'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.' My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

The critical fact in this case is that '(o)ne who occupies it, (a telephone booth) shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted. The point is not that the booth is 'accessible to the public' at other times, but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable.

Justice BLACK, dissenting.

I do not deny that common sense requires and that this Court often has said that the Bill of Rights' safeguards should be given a liberal construction. This principle, however, does not justify construing the search and seizure amendment as applying to eavesdropping or the 'seizure' of conversations. The Fourth Amendment was aimed directly at the abhorred practice of breaking in, ransacking and searching homes and other buildings and seizing people's personal belongings without warrants issued by magistrates. The Amendment deserves, and this Court has given it, a liberal construction in order to protect against warrantless searches of buildings and seizures of tangible personal effects. But until today this Court has refused to say that eavesdropping comes within the ambit of Fourth Amendment restrictions.

Since I see no way in which the words of the Fourth Amendment can be construed to apply to eavesdropping, that closes the matter for me. In interpreting the Bill of Rights, I willingly go as far as a liberal construction of the language takes me, but I simply cannot in good conscience give a meaning to words which they have never before been thought to have and which they certainly do not have in common ordinary usage. I will not distort the words of

the Amendment in order to 'keep the Constitution up to date' or 'to bring it into harmony with the times.' It was never meant that this Court have such power, which in effect would make us a continuously functioning constitutional convention.

Notes

1. In his concurrence, Harlan wrote that police conduct amounts to a search, thereby implicating the Fourth Amendment, when "a person [exhibits] an actual (subjective) expectation of privacy, and [when] the expectation [is] one that society is prepared to recognize as 'reasonable.'" In subsequent cases, the Court has embraced this test and it has become the touchstone for determining whether surveillance constitutes a "search" within the meaning of the Fourth Amendment. Thus, for over fifty years courts have spoken of "reasonable expectations of privacy."
2. The exact meaning of "reasonable expectations of privacy" has proven elusive. Some social-science-minded scholars have argued that it should be thought of in terms of the expectations of reasonable people. Christopher Slobogin and Joseph Schumacher pioneered this method by having respondents rate the intrusiveness of a variety of law enforcement information-gathering techniques.[76] Though they largely found respondents' opinions typically track judicial conclusions about whether the technique at issue constitutes a "search" under the Fourth Amendment, scattered and important divergences do arise. In general, the theme of this work is that regular people expect more privacy than courts have historically been inclined to grant them.[77]
3. Whether one takes a normative or descriptive approach to reasonable expectations of privacy, one should recognize the number of hard questions raised by this test. In most areas of law, reasonableness is highly context dependent. This means that it is fair to wonder how the reasonableness of endless hypotheticals would be assessed. Is it reasonable to expect privacy when at a table in a restaurant? Reasonable to expect privacy against a hidden bug, but not against a neighboring diner? Reasonable only if the restaurant is relatively empty?

Though *Katz* drastically changed Fourth Amendment law in many areas, one issue it left untouched was the misplaced trust doctrine. As we shall see, this doctrine has substantial implications as it is applied to data in subsequent decades.

United States v. White, 401 U.S. 745 (1971)

Justice WHITE announced the judgment of the Court and an opinion in which THE CHIEF JUSTICE, STEWART, and BLACKMUN join.

In 1966, respondent James A. White was tried and convicted under two consolidated indictments charging various illegal transactions in narcotics. The issue before us is whether the Fourth Amendment bars from evidence the testimony of governmental agents who related certain conversations which had occurred between defendant White and a government informant, Harvey Jackson, and which the agents overheard by monitoring the frequency of a radio transmitter carried by Jackson and concealed on his person. On four occasions the

---

[76] Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727 (1993).

[77] For an extensive discussion of the doctrinal basis for using such data, see Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, SUP. Ct. REV. 205, 207–09 (2015). For other examples of this kind of work, see Christine S. Scott-Hayward, Henry F. Fradella & Ryan G. Fischer, *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 45–58 (2015); Bernard Chao, Catherine Durso, Ian Farrell & Christopher Robertson, *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263, 297–315 (2018).

conversations took place in Jackson's home; each of these conversations was overheard by an agent concealed in a kitchen closet with Jackson's consent and by a second agent outside the house using a radio receiver. Four other conversations—one in respondent's home, one in a restaurant, and two in Jackson's car—were overheard by the use of radio equipment. The prosecution was unable to locate and produce Jackson at the trial and the trial court overruled objections to the testimony of the agents who conducted the electronic surveillance. The jury returned a guilty verdict and defendant appealed.

Katz v. United States . . . swept away doctrines that electronic eavesdropping is permissible under the Fourth Amendment unless physical invasion of a constitutionally protected area produced the challenged evidence. The Court of Appeals understood *Katz* to render inadmissible against White the agents' testimony concerning conversations that Jackson broadcast to them. We cannot agree. *Katz* involved no revelation to the Government by a party to conversations with the defendant nor did the Court indicate in any way that a defendant has a justifiable and constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police.

Hoffa v. United States (1966), which was left undisturbed by *Katz*, held that however strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities. In these circumstances, 'no interest legitimately protected by the Fourth Amendment is involved,' for that amendment affords no protection to 'a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.' No warrant to 'search and seize' is required in such circumstances, nor is it when the Government sends to defendant's home a secret agent who conceals his identity and makes a purchase of narcotics from the accused or when the same agent, unbeknown to the defendant, carries electronic equipment to record the defendant's words and the evidence so gathered is later offered in evidence.

Concededly a police agent who conceals his police connections may write down for official use his conversations with a defendant and testify concerning them, without a warrant authorizing his encounters with the defendant and without otherwise violating the latter's Fourth Amendment rights. For constitutional purposes, no different result is required if the agent instead of immediately reporting and transcribing his conversations with defendant, either (1) simultaneously records them with electronic equipment which he is carrying on his person, (2) or carries radio equipment which simultaneously transmits the conversations either to recording equipment located elsewhere or to other agents monitoring the transmitting frequency. If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks.

Our problem is not what the privacy expectations of particular defendants in particular situations may be or the extent to which they may in fact have relied on the discretion of their companions. Very probably, individual defendants neither know nor suspect that their colleagues have gone or will go to the police or are carrying recorders or transmitters. Otherwise, conversation would cease and our problem with these encounters would be nonexistent or far different from those now before us.

Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his. In terms of what his course will be, what he will or will not do or say, we are unpersuaded that he would distinguish between probably informers on the one hand and probable informers with transmitters on the other.

Nor should we be too ready to erect constitutional barriers to relevant and probative evidence which is also accurate and reliable. An electronic recording will many times produce a more reliable rendition of what a defendant has said than will the unaided memory of a police agent. It may also be that with the recording in existence it is less likely that the informant will change his mind, less chance that threat or injury will suppress unfavorable evidence and less chance that cross-examination will confound the testimony. Considerations like these obviously do not favor the defendant, but we are not prepared to hold that a defendant who has no constitutional right to exclude the informer's unaided testimony nevertheless has a Fourth Amendment privilege against a more accurate version of the events in question.

No different result should obtain where . . . the informer disappears and is unavailable at trial; for the issue of whether specified events on a certain day violate the Fourth Amendment should not be determined by what later happens to the informer. His unavailability at trial and proffering the testimony of other agents may raise evidentiary problems or pose issues of prosecutorial misconduct with respect to the informer's disappearance, but they do not appear critical to deciding whether prior events invaded the defendant's Fourth Amendment rights.

Justice DOUGLAS, dissenting.

Today no one perhaps notices because only a small, obscure criminal is the victim. But every person is the victim, for the technology we exalt today is everyman's master. Any doubters should read Arthur R. Miller's *The Assault on Privacy* (1971). After describing the monitoring of conversations and their storage in data banks, Professor Miller goes on to describe 'human monitoring' which he calls the 'ultimate step in mechanical snooping'—a device for spotting unorthodox or aberrational behavior across a wide spectrum. 'Given the advancing state of both the remote sensing art and the capacity of computers to handle an uninterrupted and synoptic data flow, there seem to be no physical barriers left to shield us from intrusion.'

Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances. Free discourse—a First Amendment value—may be frivolous or serious, humble or defiant, reactionary or revolutionary, profane or in good taste; but it is not free if there is surveillance. Free discourse liberates the spirit, though it may produce only froth. The individual must keep some facts concerning his thoughts within a small zone of people. At the same time he must be free to pour out his woes or inspirations or dreams to others. He remains the sole judge as to what must be said and what must remain unspoken. This is the essence of the idea of privacy implicit in the First and Fifth Amendments as well as in the Fourth.

Few conversations would be what they are if the speakers thought others were listening. Silly, secret, thoughtless and thoughtful statements would all be affected. The sheer numbers in our lives, the anonymity of urban living and the inability to influence things that are important are depersonalizing and dehumanizing factors of modern life. To penetrate the last refuge of the individual, the precious little privacy that remains, the basis of individual dignity, can have meaning to the quality of our lives that we cannot foresee. In terms of present values, that meaning cannot be good.

[M]ust everyone live in fear that every word he speaks may be transmitted or recorded and later repeated to the entire world? I can imagine nothing that has a more chilling effect on people speaking their minds and expressing their views on important matters. The advocates of that regime should spend some time in totalitarian countries and learn firsthand the kind of regime they are creating here.

Notes

1. Another issue in the *White* case concerned timing. The monitoring in *White* preceded the Court's decision in *Katz*, and *Katz* was held not to be retrospective. This made the appellate court's reliance on *Katz* misplaced in the eyes of some of the Justices, contributing to the fracturing of the Court. Consider how the modern good-faith exception would treat this

argument. Is it right to effectively gloss over something that was later determined to be a constitutional violation?
2. Is Justice White correct in minimizing the difference between an informant recording a conversation and the informant testifying about the conversation? Is there a principled way of differentiating between the two cases? Think back to privacy torts. Photos are often believed to be different than memories and words in that context.
3. Sometimes informants testify falsely. Are we better off with more recording of informant interactions as opposed to less? This plays into perennial debates about the merits of police body cameras and recorded police interrogations.

2) The Third-Party Doctrine

The basic insight of *White* leads directly into the problem of third-party records. In addition to trusting our friends, lovers, and criminal co-conspirators, we also trust a variety of other actors. Specifically, we trust our banks, our internet search companies, our telecommunications providers, and our hardware store clerks. Do we have any constitutional privacy expectations in the information they hold about us in their own books and ledgers? In a word, no. And that has vast implications for our increasingly digital and connected world.

Smith v. Maryland, 442 U.S. 735 (1979)

Justice BLACKMUN delivered the opinion of the Court.

This case presents the question whether the installation and use of a pen register[1] constitutes a "search" within the meaning of the Fourth Amendment.

On March 5, 1976, in Baltimore, Md., Patricia McDonough was robbed. She gave the police a description of the robber and of a 1975 Monte Carlo automobile she had observed near the scene of the crime. After the robbery, McDonough began receiving threatening and obscene phone calls from a man identifying himself as the robber. On one occasion, the caller asked that she step out on her front porch; she did so, and saw the 1975 Monte Carlo she had earlier described to police moving slowly past her home. On March 16, police spotted a man who met McDonough's description driving a 1975 Monte Carlo in her neighborhood. By tracing the license plate number, police learned that the car was registered in the name of petitioner, Michael Lee Smith.

The next day, the telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at petitioner's home. The police did not get a warrant or court order before having the pen register installed. The register revealed that on March 17 a call was placed from petitioner's home to McDonough's phone. On the basis of this and other evidence, the police obtained a warrant to search petitioner's residence. The search revealed that a page in petitioner's phone book was turned down to the name and number of Patricia McDonough; the phone book was seized. Petitioner was arrested, and a six-man lineup was held on March 19. McDonough identified petitioner as the man who had robbed her.

Petitioner was indicted in the Criminal Court of Baltimore for robbery. By pretrial motion, he sought to suppress "all fruits derived from the pen register" on the ground that the

[1] "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." *United States v. New York Tel. Co.* (1977). A pen register is "usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line" to which it is attached. *United States v. Giordano* (1974).

police had failed to secure a warrant prior to its installation. The trial court denied the suppression motion, holding that the warrantless installation of the pen register did not violate the Fourth Amendment.

The Court of Appeals affirmed the judgment of conviction, holding that "there is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the fourth amendment is implicated by the use of a pen register installed at the central offices of the telephone company.

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." In determining whether a particular form of government-initiated electronic surveillance is a "search" within the meaning of the Fourth Amendment,[4] our lodestar is *Katz v. United States,* (1967). The Court rejected the argument that a "search" can occur only when there has been a "physical intrusion" into a "constitutionally protected area," noting that the Fourth Amendment "protects people, not places." Because the Government's monitoring of Katz' conversation "violated the privacy upon which he justifiably relied while using the telephone booth," the Court held that it "constituted a 'search and seizure' within the meaning of the Fourth Amendment."

Consistently with *Katz,* this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a "justifiable," a "reasonable," or a "legitimate expectation of privacy" that has been invaded by government action. This inquiry, as Mr. Justice Harlan aptly noted in his *Katz* concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy"—whether, in the words of the *Katz* majority, the individual has shown that "he seeks to preserve [something] as private." The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable,'"—whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is "justifiable" under the circumstances.[5]

In applying the *Katz* analysis to this case, it is important to begin by specifying precisely the nature of the state activity that is challenged. The activity here took the form of installing and using a pen register. Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his "property" was invaded or that police intruded into a "constitutionally protected area." Petitioner's claim, rather, is that, notwithstanding the absence of a trespass, the State, as did the Government in *Katz*, infringed a "legitimate expectation of privacy" that petitioner held. Yet a pen register

---

[4] In this case, the pen register was installed, and the numbers dialed were recorded, by the telephone company. The telephone company, however, acted at police request. In view of this, respondent appears to concede that the company is to be deemed an "agent" of the police for purposes of this case, so as to render the installation and use of the pen register "state action" under the Fourth and Fourteenth Amendments. We may assume that "state action" was present here.

[5] Situations can be imagined, of course, in which *Katz'* two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.

differs significantly from the listening device employed in *Katz,* for pen registers do not acquire the *contents* of communications. This Court recently noted:

"Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."

Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone.

This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud and preventing violations of law." Electronic equipment is used not only to keep billing records of toll calls, but also "to keep a record of all calls dialed from a telephone which is subject to a special rate structure." Pen registers are regularly employed "to determine whether a home phone is being used to conduct a business, to check for a defective dial, or to check for overbilling." Although most people may be oblivious to a pen register's esoteric functions, they presumably have some awareness of one common use: to aid in the identification of persons making annoying or obscene calls. Most phone books tell subscribers, on a page entitled "Consumer Information," that the company "can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls." Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.

Petitioner argues, however, that, whatever the expectations of telephone users in general, he demonstrated an expectation of privacy by his own conduct here, since he "us[ed] the telephone *in his house* to the exclusion of all others." But the site of the call is immaterial for purposes of analysis in this case. Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.

Second, even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not "one that society is prepared to recognize as 'reasonable.'" This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. In *United States v. Miller* (1976), for example, the Court held that a bank depositor has no "legitimate 'expectation of privacy'" in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business." The Court explained:

> "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

Because the depositor "assumed the risk" of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.

This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.

Petitioner argues, however, that automatic switching equipment differs from a live operator in one pertinent respect. An operator, in theory at least, is capable of remembering every number that is conveyed to him by callers. Electronic equipment, by contrast can "remember" only those numbers it is programmed to record, and telephone companies, in view of their present billing practices, usually do not record local calls. Since petitioner, in calling McDonough, was making a local call, his expectation of privacy as to her number, on this theory, would be "legitimate."

This argument does not withstand scrutiny. The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police. Under petitioner's theory, Fourth Amendment protection would exist, or not, depending on how the telephone company chose to define local-dialing zones, and depending on how it chose to bill its customers for local calls. Calls placed across town, or dialed directly, would be protected; calls placed across the river, or dialed with operator assistance, might not be. We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.

We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not "legitimate." The installation and use of a pen register, consequently, was not a "search," and no warrant was required. The judgment of the Maryland Court of Appeals is affirmed.

Justice STEWART, with whom BRENNAN joins, dissenting.

I think that the numbers dialed from a private telephone—like the conversations that occur during a call—are within the constitutional protection recognized in *Katz*. The information captured by such surveillance emanates from private conduct within a person's home or office—locations that without question are entitled to Fourth and Fourteenth Amendment protection. Further, that information is an integral part of the telephonic communication that under *Katz* is entitled to constitutional protection, whether or not it is captured by a trespass into such an area.

The numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without "content." Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long-distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.

Justice MARSHALL, with whom BRENNAN joins, dissenting.

Implicit in the concept of assumption of risk is some notion of choice. At least in the third-party consensual surveillance cases, which first incorporated risk analysis into Fourth Amendment doctrine, the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications. By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of "assuming" risks in contexts where, as a practical matter, individuals have no realistic alternative.

More fundamentally, to make risk analysis dispositive in assessing the reasonableness of privacy expectations would allow the government to define the scope of Fourth Amendment protections. For example, law enforcement officials, simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations, could put the public on notice of the risks they would thereafter assume in such communications. Yet, although acknowledging this implication of its analysis, the Court is willing to concede only that, in some circumstances, a further "normative inquiry would be proper." No meaningful effort is made to explain what those circumstances might be, or why this case is not among them.

Notes

1. There is a lot going on in *Smith*. Most centrally, this case establishes that there is no constitutional expectation of privacy in most third-party business records. You cannot invoke Fourth Amendment protection to prevent stores where you shop, apps that you install, and people with whom you speak with from disclosing your secrets. Sometimes statutes gap-fill in this area—see, for example, the below section on the Stored Communications Act. But other times no privacy protection is extended by either statute or the Constitution.
2. Under the third-party doctrine, people do not have a reasonable expectation of privacy in most information voluntarily disclosed to another. Lower federal courts have applied this doctrine to power records produced by utility companies, to records kept by internet service providers, and to credit card information.
3. In footnote 5, *Smith* also raises the question of whether Fourth Amendment privacy expectations are circular. Presumably people learn from experience. If the government—either through executive announcement or judicial fiat—repeatedly tells people that they have no expectation of privacy in X or Y, it would be only natural for them to learn that. What reasonable person would expect privacy after having been told not to? It turns out that many people, reasonable or not, would still expect privacy. Scholars have repeatedly found that people expect privacy in contexts where courts have told them that they do not have it.[78] My own work, with Lior Strahilevitz, has found that even well-publicized court decisions barely change privacy expectations, and that those changes are fleeting.[79] Follow-

[78] *See* Slobogin & Schumacher, *supra* note 76.

[79] Matthew B. Kugler & Lior J. Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. 1747, 1780 (2017) (showing that privacy expectations in electronic devices increased slightly one week after a relevant ruling, but had returned to baseline one year later, and that privacy expectations in physical searches—not covered by the ruling—did not change).

up work showed that attitudes towards law enforcement surveillance also changed little over the five-year period from 2015 to 2020.[80] Does this make you more comfortable in relying on public privacy expectations? Or does this apparent ignorance argue against taking the public seriously?

4. Although *Smith* limits Fourth Amendment protections for information shared with third parties, Congress was not precluded from creating additional protections. The Right to Financial Privacy Act of 1978 prohibited government authorities from accessing the information contained in financial records without customer authorization absent an administrative subpoena, judicial subpoena, search warrant, or formal request. The requirements for some of these are not especially burdensome, but they do exist. For example, the government can only issue an administrative subpoena for financial records if the records sought are "relevant to a legitimate law enforcement inquiry" and a copy of the subpoena is delivered to the customer or their last known mailing address "on or before the date" it is served on the financial institution. The consumer then has a period of ten days from service (or fourteen days from mailing) to object in court before the records are furnished. Do you think that these additional protections are warranted for financial records? If so, do you think broader protections should apply to all data that third parties collect?

B. Constitutional limitations and new technologies

In his dissent in *Katz*, Justice Black wrote that he did not want to update the Fourth Amendment; he thought the amendment was best focused on the kind of physical intrusions that were its historical foundation. But that perspective did not win the day. So, if courts are to update the Fourth Amendment, how are they to do so?

Broadly speaking, this question has been asked in two distinct domains. One is evolving surveillance technology. What do we make of the government's ever-growing ability to monitor things without touching them? This parallels *Katz* itself. Recall that the government did not need to touch Katz, or his possessions, to monitor him.

The other domain is third-party data. In a world where data is hard to collect and expensive to store, there will be comparatively little of it. A department store in the 1980s could not state who bought what item last week. But that is not the world we now live in. Customer loyalty accounts track every purchase, and online merchants automatically generate records stretching back decades. Does this change how we should think about third-party records?

---

[80] Matthew B. Kugler & Mariana Oliver, *Constitutional Pandemic Surveillance*, 111 J. CRIM. L. & CRIMINOLOGY 909, 935–936 (2021). In addition to the lack of change in views of law enforcement surveillance over a five-year period, there was also a lack of change between April and June of 2020 itself. This may be surprising to some given that George Floyd died in May 2020 and there was a nationwide series of anti-police protests underway as the second wave of data was collected. Further, views of COVID surveillance also did not change between early April and mid-June of 2020 even as quite a lot happened in that domain as well.

1) Changing surveillance and communication technologies

First, we will consider the problem of changing surveillance technology. It has long been understood that anything in plain view of law enforcement can be observed free of Fourth Amendment scrutiny. It is hardly the fault of the police if you leave your curtains open and expose your collection of illegal weapons to their view. But what about a world in which curtains are insufficient to guard what goes on behind private walls?

Kyllo v. United States, 533 U.S. 27 (2001)

Justice SCALIA delivered the opinion of the Court.

This case presents the question whether the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a "search" within the meaning of the Fourth Amendment.

In 1991 Agent William Elliott of the United States Department of the Interior came to suspect that marijuana was being grown in the home belonging to petitioner Danny Kyllo. Indoor marijuana growth typically requires high-intensity lamps. In order to determine whether an amount of heat was emanating from petitioner's home consistent with the use of such lamps, at 3:20 a.m. on January 16, 1992, Agent Elliott and Dan Haas used an Agema Thermovision 210 thermal imager to scan the triplex. Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye. The imager converts radiation into images based on relative warmth—black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images. The scan of Kyllo's home took only a few minutes and was performed from the passenger seat of Agent Elliott's vehicle across the street from the front of the house and also from the street in back of the house. The scan showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex. Agent Elliott concluded that petitioner was using halide lights to grow marijuana in his house, which indeed he was. Based on tips from informants, utility bills, and the thermal imaging, a Federal Magistrate Judge issued a warrant authorizing a search of petitioner's home, and the agents found an indoor growing operation involving more than 100 plants. Petitioner was indicted on one count of manufacturing marijuana, in violation of 21 U.S.C. § 841(a)(1). He unsuccessfully moved to suppress the evidence seized from his home and then entered a conditional guilty plea.

The Court of Appeals for the Ninth Circuit remanded the case for an evidentiary hearing regarding the intrusiveness of thermal imaging. On remand the District Court found that the Agema 210 "is a non-intrusive device which emits no rays or beams and shows a crude visual image of the heat being radiated from the outside of the house"; it "did not show any people or activity within the walls of the structure"; "[t]he device used cannot penetrate walls or windows to reveal conversations or human activities"; and "[n]o intimate details of the home were observed."

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." "At the very core" of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."

On the other hand, the antecedent question whether or not a Fourth Amendment "search" has occurred is not so simple under our precedent. The permissibility of ordinary visual surveillance of a home used to be clear because, well into the 20th century, our Fourth

Amendment jurisprudence was tied to common-law trespass. See, *e.g., Goldman v. United States* (1942); *Olmstead v. United States* (1928). Visual surveillance was unquestionably lawful because "'the eye cannot by the laws of England be guilty of a trespass.'" *Boyd v. United States* (1886). We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property, but the lawfulness of warrantless visual surveillance of a home has still been preserved. As we observed in *California v. Ciraolo* (1986), "[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."

The present case involves officers on a public street engaged in more than naked-eye surveillance of a home. We have previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage point, if any, is too much. While we upheld enhanced aerial photography of an industrial complex in *Dow Chemical Co. v. United States* (1986), we noted that we found "it important that this is *not* an area immediately adjacent to a private home, where privacy expectations are most heightened."

It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.

We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area" constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search.

The Government maintains, however, that the thermal imaging must be upheld because it detected "only heat radiating from the external surface of the house." The dissent makes this its leading point, contending that there is a fundamental difference between what it calls "off-the-wall" observations and "through-the-wall surveillance." But just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house. We rejected such a mechanical interpretation of the Fourth Amendment in *Katz,* where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development. The dissent's reliance on the distinction between "off-the-wall" and "through-the-wall" observation is entirely incompatible with the dissent's belief, which we discuss below, that thermal-imaging observations of the intimate details of a home are impermissible. The most sophisticated thermal-imaging devices continue to measure heat "off-the-wall" rather than "through-the-wall"; the dissent's disapproval of those more sophisticated thermal-imaging devices, is an acknowledgement that there is no substance to this distinction. As for the dissent's extraordinary assertion that anything learned through "an inference" cannot be a search, that would validate even the "through-the-wall" technologies that the dissent purports to disapprove. Surely the dissent does not believe that the through-the-wall radar or ultrasound technology produces an 8–by–10 Kodak glossy that needs no analysis (*i.e.,* the making of inferences).

Limiting the prohibition of thermal imaging to "intimate details" would not only be wrong in principle; it would be impractical in application . . . . To begin with, there is no necessary connection between the sophistication of the surveillance equipment and the

"intimacy" of the details that it observes—which means that one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful. The Agema Thermovision 210 might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider "intimate"; and a much more sophisticated system might detect nothing more intimate than the fact that someone left a closet light on.

Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.

Justice STEVENS, with whom THE CHIEF, O'CONNOR, and KENNEDY join dissenting.

There is, in my judgment, a distinction of constitutional magnitude between "through-the-wall surveillance" that gives the observer or listener direct access to information in a private area, on the one hand, and the thought processes used to draw inferences from information in the public domain, on the other hand. The Court has crafted a rule that purports to deal with direct observations of the inside of the home, but the case before us merely involves indirect deductions from "off-the-wall" surveillance, that is, observations of the exterior of the home. Those observations were made with a fairly primitive thermal imager that gathered data exposed on the outside of petitioner's home but did not invade any constitutionally protected interest in privacy. Moreover, I believe that the supposedly "bright-line" rule the Court has created in response to its concerns about future technological developments is unnecessary, unwise, and inconsistent with the Fourth Amendment.

Notwithstanding the implications of today's decision, there is a strong public interest in avoiding constitutional litigation over the monitoring of emissions from homes, and over the inferences drawn from such monitoring. Just as "the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public" *Greenwood*, so too public officials should not have to avert their senses or their equipment from detecting emissions in the public domain such as excessive heat, traces of smoke, suspicious odors, odorless gases, airborne particulates, or radioactive emissions, any of which could identify hazards to the community. In my judgment, monitoring such emissions with "sense-enhancing technology," and drawing useful conclusions from such monitoring, is an entirely reasonable public service.

Notes

1. Is the "general public use" standard workable given the rapid pace of technological advancement? Drones are now relatively cheap, and thermal sensors are readily available in hardware stores. Does use of the specific technology in *Kyllo* still represent a Fourth Amendment search if it can be purchased from Home Depot for $200?
2. What about other ways of obtaining the same information the government wanted in *Kyllo*? Courts repeatedly held that accessing utility records to find excess power consumption—another sign of home marijuana cultivation—did not require a warrant. See e.g., *United States v. Golden Valley Elec. Ass'n*, 689 F.3d 1108 (9th Cir. 2012). Is accessing that kind of third-party record fundamentally different than observing "off-the-wall" emissions?

Kyllo was the leading case on the Fourth Amendment and technological change for a number of years. Ultimately, it was supplanted by *United States v. Jones* (2012) and *Carpenter v. United States* (2018), which you will read later in this chapter. Collectively, these cases show that courts felt the need to account for rapidly changing technology.

One way of coping with technological change is through analogy. This is exemplified by the Sixth Circuit's opinion in *United States v. Warshak* (6th Cir. 2010), which follows and holds

that a warrant is required to obtain email content. If you are wondering why you are reading circuit-level salami sandwiched between so many layers of Supreme Court bread, it is because the Supreme Court has never actually ruled on the question of email privacy. Further, there is no circuit split on the issue and the Department of Justice subsequently conceded that a warrant is required for email content, so there likely never will be an explicit Supreme Court holding.

When reading *Warshak*, it is helpful to recognize the several revolutions in communications technology. From 1800 to the present, we have seen the rise and fall of telegraphs, the transition to landline phones, the transition to cellular phones, and finally the gradual transition to using phones as general electronic messaging devices. Each of these changes has carried with it changes in social convention. Telegraph messages were transmitted by professional operators, from whom the contents of the messages could not be concealed. Phones too were originally intermediary-intensive, with operators manually connecting calls and occasionally even call contents being relayed by others. Then every house had its own phone and all connections were made automatically. Now phones are more pervasive and nearly every person has their own.

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)

BOGGS, Circuit Judge.

Berkeley Premium Nutraceuticals, Inc., was an incredibly profitable company that served as the distributor of Enzyte, an herbal supplement purported to enhance male sexual performance. In this appeal, defendants Steven Warshak ("Warshak"), Harriet Warshak ("Harriet"), and TCI Media, Inc. ("TCI"), challenge their convictions stemming from a massive scheme to defraud Berkeley's customers.

Before trial, numerous motions were filed. First, Warshak moved to exclude thousands of emails that the government obtained from his Internet Service Providers. That motion was denied.

Warshak argues that the government's warrantless, *ex parte* seizure of approximately 27,000 of his private emails constituted a violation of the Fourth Amendment's prohibition on unreasonable searches and seizures. The government counters that, even if government agents violated the Fourth Amendment in obtaining the emails, they relied in good faith on the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 et seq., a statute that allows the government to obtain certain electronic communications without procuring a warrant. We find that the government *did* violate Warshak's Fourth Amendment rights by compelling his Internet Service Provider ("ISP") to turn over the contents of his emails. However, we agree that agents relied on the SCA in good faith, and therefore hold that reversal is unwarranted.

Email was a critical form of communication among Berkeley personnel. As a consequence, Warshak had a number of email accounts with various ISPs, including an account with NuVox Communications. In October 2004, the government formally requested that NuVox prospectively preserve the contents of any emails to or from Warshak's email account. The request was made pursuant to 18 U.S.C. § 2703(f) and it instructed NuVox to preserve all future messages.[14] NuVox acceded to the government's request and began preserving copies of Warshak's incoming and outgoing emails—copies that would not have existed absent the prospective preservation request. Per the government's instructions, Warshak was not informed that his messages were being archived.

---

[14] Warshak appears to have accessed emails from his NuVox account via POP, or "Post Office Protocol." When POP is utilized, emails are downloaded to the user's personal computer and generally deleted from the ISP's server.

In January 2005, the government obtained a subpoena under § 2703(b) and compelled NuVox to turn over the emails that it had begun preserving the previous year. In May 2005, the government served NuVox with an *ex parte* court order under § 2703(d) that required NuVox to surrender any additional email messages in Warshak's account. In all, the government compelled NuVox to reveal the contents of approximately 27,000 emails. Warshak did not receive notice of either the subpoena or the order until May 2006.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ." U.S. CONST. amend. IV. The fundamental purpose of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials."

Not all government actions are invasive enough to implicate the Fourth Amendment. "The Fourth Amendment's protections hinge on the occurrence of a 'search,' a legal term of art whose history is riddled with complexity." A "search" occurs when the government infringes upon "an expectation of privacy that society is prepared to consider reasonable." This standard breaks down into two discrete inquiries: "first, has the [target of the investigation] manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?"

Turning first to the subjective component of the test, we find that Warshak plainly manifested an expectation that his emails would be shielded from outside scrutiny. As he notes in his brief, his "entire business and personal life was contained within the . . . emails seized." Given the often sensitive and sometimes damning substance of his emails, we think it highly unlikely that Warshak expected them to be made public, for people seldom unfurl their dirty laundry in plain view. Therefore, we conclude that Warshak had a subjective expectation of privacy in the contents of his emails.

The next question is whether society is prepared to recognize that expectation as reasonable. *See Smith v. Maryland* (1979). This question is one of grave import and enduring consequence, given the prominent role that email has assumed in modern communication. Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities. Much hinges, therefore, on whether the government is permitted to request that a commercial ISP turn over the contents of a subscriber's emails without triggering the machinery of the Fourth Amendment.

In confronting this question, we take note of two bedrock principles. First, the very fact that information is being passed through a communications network is a paramount Fourth Amendment consideration. Second, the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish. *See Kyllo v. United States* (2001) (noting that evolving technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment").

With those principles in mind, we begin our analysis by considering the manner in which the Fourth Amendment protects traditional forms of communication. In *Katz,* the Supreme Court was asked to determine how the Fourth Amendment applied in the context of the telephone. There, government agents had affixed an electronic listening device to the exterior

of a public phone booth, and had used the device to intercept and record several phone conversations. The Supreme Court held that this constituted a search under the Fourth Amendment, notwithstanding the fact that the telephone company had the capacity to monitor and record the calls. In the eyes of the Court, the caller was "surely entitled to assume that the words he utter[ed] into the mouthpiece w[ould] not be broadcast to the world." The Court's holding in *Katz* has since come to stand for the broad proposition that, in many contexts, the government infringes a reasonable expectation of privacy when it surreptitiously intercepts a telephone call through electronic means.

Letters receive similar protection. *See United States v. Jacobsen* (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy."). While a letter is in the mail, the police may not intercept it and examine its contents unless they first obtain a warrant based on probable cause. This is true despite the fact that sealed letters are handed over to perhaps dozens of mail carriers, any one of whom could tear open the thin paper envelopes that separate the private words from the world outside. Put another way, trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private.

Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection. Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age. Over the last decade, email has become "so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[ ] for self-expression, even self-identification." It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve. As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise.

If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company. As we have discussed above, the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call—unless they get a warrant, that is.

In *Warshak I,* the government argued that this conclusion was improper, pointing to the fact that NuVox contractually reserved the right to access Warshak's emails for certain purposes. While we acknowledge that a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account, we doubt that will be the case in most situations, and it is certainly not the case here.

As an initial matter, it must be observed that the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy. In *Katz,* the Supreme Court found it reasonable to expect privacy during a telephone call despite the ability of an operator to listen in. Similarly, the ability of a rogue mail handler to rip open a letter does not make it unreasonable to assume that sealed mail will remain private on its journey across the country. Therefore, the threat or possibility of access is not decisive when it comes to the reasonableness of an expectation of privacy.

Nor is the *right* of access. As the Electronic Frontier Foundation points out in its *amicus* brief, at the time *Katz* was decided, telephone companies had a right to monitor calls in certain situations. Specifically, telephone companies could listen in when reasonably necessary to

"protect themselves and their properties against the improper and illegal use of their facilities." *Bubis v. United States* (9th Cir. 1967). In this case, the NuVox subscriber agreement tracks that language, indicating that "NuVox *may* access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service." Thus, under *Katz*, the degree of access granted to NuVox does not diminish the reasonableness of Warshak's trust in the privacy of his emails.

Again, however, we are unwilling to hold that a subscriber agreement will *never* be broad enough to snuff out a reasonable expectation of privacy. As the panel noted in *Warshak I*, if the ISP expresses an intention to "audit, inspect, and monitor" its subscriber's emails, that might be enough to render an expectation of privacy unreasonable.

We recognize that our conclusion may be attacked in light of the Supreme Court's decision in *United States v. Miller* (1976). In *Miller*, the Supreme Court held that a bank depositor does not have a reasonable expectation of privacy in the contents of bank records, checks, and deposit slips.

But *Miller* is distinguishable. First, *Miller* involved simple business records, as opposed to the potentially unlimited variety of "confidential communications" at issue here. Second, the bank depositor in *Miller* conveyed information to the bank so that the bank could put the information to use "in the ordinary course of business." By contrast, Warshak received his emails through NuVox. NuVox was an *intermediary*, not the intended recipient of the emails. Thus, *Miller* is not controlling. Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails.

Even though the government's search of Warshak's emails violated the Fourth Amendment, the emails are not subject to the exclusionary remedy if the officers relied in good faith on the SCA to obtain them. Consequently, we find that, although the government violated the Fourth Amendment, the exclusionary rule does not apply, as the government relied in good faith on § 2703(b) and § 2703(d) to access the contents of Warshak's emails.[22]

Notes

1. Despite setting a massively important pro-privacy precedent, Warshak still loses. This is a common occurrence in Fourth Amendment cases and may explain why courts are so willing to extend privacy protections—they can often do so secure in the knowledge that the accused offender in front of them will still be convicted.
2. The *Warshak* case is surprising if one takes seriously email-content scanning, which was then at its height. Google was famous for its keyword scanning of user emails to better target advertising. One could have expected this case to lead to a line-by-line scanning of provider privacy policies—to what extent is each provider reserving the right to monitor email? Perhaps Proton Mail should require a warrant, but Gmail not. Instead, however, we get a near bright-line rule. Email is mail and should be treated as such. Content is protected unless there is an extremely clear provision that content is not private. Notably, Google later abandoned its practice of scanning email content for targeted advertising. This may indicate that the private sector is also coming to view email as closer to mail.
3. Under *Warshak*, only email content is protected, not email-addressing information. This is the content–envelope distinction. As a physical address is printed on the outside of an envelope and is visible to the mail carrier, so too is email addressing information. This division between content information (protected) and metadata information (not protected)

[22] In addition, we note that the Fourth Amendment violation was likely harmless. The NuVox emails did not play a role in obtaining the search warrant that produced the overwhelming majority of the evidence in this case. In addition, only three of the emails were introduced at trial, and they were largely cumulative of the testimony of William Bertemes, Warshak's accountant.

is hugely important in the context of the Electronic Communications Privacy Act, described below.

2) Location Tracking

If *Kyllo* concerns piercing the walls of the home and *Warshak* concerns the kind of electronic messages one can send from the home, *Jones* and *Carpenter* concern what happens when you leave your home. A suspect's physical location is essential to solving many crimes. If a person is murdered at location A, one can be relatively sure that the murderer was at location A at the same time. If a store is robbed at 5:01 PM, investigators should generally discount as a suspect anyone who was on the other side of town around the same time. While physical location is less important in the domain of cyber offenses, even now much crime is physical and in-person. For the investigation of such offenses, location information is crucial.

United States v. Jones, 565 U.S. 400 (2012)

Justice SCALIA delivered the opinion of the Court.

We decide whether the attachment of a Global–Positioning–System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment.

I

In 2004 respondent Antoine Jones, owner and operator of a nightclub in the District of Columbia, came under suspicion of trafficking in narcotics and was made the target of an investigation by a joint Federal Bureau of Investigation and Metropolitan Police Department task force. Officers employed various investigative techniques, including visual surveillance of the nightclub, installation of a camera focused on the front door of the club, and a pen register and wiretap covering Jones's cellular phone.

Based in part on information gathered from these sources, in 2005 the Government applied to the United States District Court for the District of Columbia for a warrant authorizing the use of an electronic tracking device on the Jeep Grand Cherokee registered to Jones's wife. A warrant issued, authorizing installation of the device in the District of Columbia and within 10 days.

On the 11th day, and not in the District of Columbia but in Maryland,[1] agents installed a GPS tracking device on the undercarriage of the Jeep while it was parked in a public parking lot. Over the next 28 days, the Government used the device to track the vehicle's movements, and once had to replace the device's battery when the vehicle was parked in a different public lot in Maryland. By means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the 4–week period.

The Government ultimately obtained a multiple-count indictment charging Jones and several alleged co-conspirators with, as relevant here, conspiracy to distribute and possess with intent to distribute five kilograms or more of cocaine and 50 grams or more of cocaine base. Before trial, Jones filed a motion to suppress evidence obtained through the GPS device. The District Court granted the motion only in part, suppressing the data obtained while the vehicle was parked in the garage adjoining Jones's residence. It held the remaining data admissible,

[1] In this litigation, the Government has conceded noncompliance with the warrant and has argued only that a warrant was not required. *United States v. Maynard*, 615 F.3d 544, 566 (D.C. Cir. 2010).

because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."

The United States Court of Appeals for the District of Columbia Circuit reversed the conviction because of admission of the evidence obtained by warrantless use of the GPS device which, it said, violated the Fourth Amendment. *United States v. Maynard* (2010). The D.C. Circuit denied the Government's petition for rehearing en banc, with four judges dissenting. We granted certiorari.

II

A

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." It is beyond dispute that a vehicle is an "effect" as that term is used in the Amendment. We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a "search."

It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted. *Entick v. Carrington* (C.P. 1765), is a "case we have described as a 'monument of English freedom' 'undoubtedly familiar' to 'every American statesman' at the time the Constitution was adopted, and considered to be 'the true and ultimate expression of constitutional law'" with regard to search and seizure. *Brower v. County of Inyo* (1989). In that case, Lord Camden expressed in plain terms the significance of property rights in search-and-seizure analysis:

> [O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law. *Entick*.

The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to "the right of the people to be secure against unreasonable searches and seizures"; the phrase "in their persons, houses, papers, and effects" would have been superfluous.

Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century. Our later cases, of course, have deviated from that exclusively property-based approach. In *Katz v. United States* (1967), we said that "the Fourth Amendment protects people, not places," and found a violation in attachment of an eavesdropping device to a public telephone booth. Our later cases have applied the analysis of Justice Harlan's concurrence in that case, which said that a violation occurs when government officers violate a person's "reasonable expectation of privacy."

The Government contends that the Harlan standard shows that no search occurred here, since Jones had no "reasonable expectation of privacy" in the area of the Jeep accessed by Government agents (its underbody) and in the locations of the Jeep on the public roads, which were visible to all. But we need not address the Government's contentions, because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, we must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." As explained, for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ("persons, houses, papers, and effects") it enumerates. *Katz* did not repudiate that understanding. Less than two years later the Court upheld defendants' contention that the

Government could not introduce against them conversations between *other* people obtained by warrantless placement of electronic surveillance devices in their homes. The opinion rejected the dissent's contention that there was no Fourth Amendment violation "unless the conversational privacy of the homeowner himself is invaded." *Alderman v. United States* (1969). "[W]e [do not] believe that *Katz*, by holding that the Fourth Amendment protects persons and their private conversations, was intended to withdraw any of the protection which the Amendment extends to the home . . . ."

B

The concurrence begins by accusing us of applying "18th-century tort law." That is a distortion. What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection it afforded when it was adopted. The concurrence does not share that belief. It would apply *exclusively Katz* 's reasonable-expectation-of-privacy test, even when that eliminates rights that previously existed.

The concurrence faults our approach for "present[ing] particularly vexing problems" in cases that do not involve physical contact, such as those that involve the transmission of electronic signals. We entirely fail to understand that point. For unlike the concurrence, which would make *Katz* the *exclusive* test, we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.

In fact, it is the concurrence's insistence on the exclusivity of the *Katz* test that needlessly leads us into "particularly vexing problems" in the present case. This Court has to date not deviated from the understanding that mere visual observation does not constitute a search. We accordingly held in *United States v. Knotts* (1983) that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." Thus, even assuming that the concurrence is correct to say that "[t]raditional surveillance" of Jones for a 4–week period "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance," our cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.

And answering it affirmatively leads us needlessly into additional thorny problems. The concurrence posits that "relatively short-term monitoring of a person's movements on public streets" is okay, but that "the use of longer-term GPS monitoring in investigations *of most offenses* " is no good. That introduces yet another novelty into our jurisprudence. There is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated. And even accepting that novelty, it remains unexplained why a 4–week investigation is "surely" too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an "extraordinary offens[e]" which may permit longer observation. What of a 2–day monitoring of a suspected purveyor of stolen electronics? Or of a 6–month monitoring of a suspected terrorist? We may have to grapple with these "vexing problems" in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.

Justice SOTOMAYOR, concurring.

I join the Court's opinion because I agree that a search within the meaning of the Fourth Amendment occurs, at a minimum, "[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area."

Nonetheless, as Justice ALITO notes, physical intrusion is now unnecessary to many forms of surveillance. With increasing regularity, the government will be capable of duplicating

the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones.

In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, *e.g., People v. Weaver* (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." *Illinois v. Lidster* (2004).

Awareness that the government may be watching chills associational and expressive freedoms. And the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." *United States v. Cuevas-Perez* (7th Cir. 2011) (Flaum, J., concurring).

I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice ALITO notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Justice ALITO, with whom Justice GINSBURG, Justice BREYER, and Justice KAGAN join, concurring in the judgment.

This case requires us to apply the Fourth Amendment's prohibition of unreasonable searches and seizures to a 21st-century surveillance technique, the use of a Global Positioning System (GPS) device to monitor a vehicle's movements for an extended period of time. Ironically, the Court has chosen to decide this case based on 18th-century tort law. By attaching

a small GPS device to the underside of the vehicle that respondent drove, the law enforcement officers in this case engaged in conduct that might have provided grounds in 1791 for a suit for trespass to chattels. And for this reason, the Court concludes, the installation and use of the GPS device constituted a search.

This holding, in my judgment, is unwise. It strains the language of the Fourth Amendment; it has little if any support in current Fourth Amendment case law; and it is highly artificial.

I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.

The Court argues—and I agree—that "we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" But it is almost impossible to think of late–18th-century situations that are analogous to what took place in this case. (Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?[3]) The Court's theory seems to be that the concept of a search, as originally understood, comprehended any technical trespass that led to the gathering of evidence, but we know that this is incorrect. At common law, any unauthorized intrusion on private property was actionable, but a trespass on open fields, as opposed to the "curtilage" of a home, does not fall within the scope of the Fourth Amendment because private property outside the curtilage is not part of a "hous[e]" within the meaning of the Fourth Amendment.

The Court's reasoning in this case is very similar to that in the Court's early decisions involving wiretapping and electronic eavesdropping, namely, that a technical trespass followed by the gathering of evidence constitutes a search.

This trespass-based rule was repeatedly criticized. *Katz* finally did away with the old approach, holding that a trespass was not required for a Fourth Amendment violation.

Under this approach, as the Court later put it when addressing the relevance of a technical trespass, "an actual trespass is neither necessary *nor sufficient* to establish a constitutional violation." In *Oliver v. United States* (1984), the Court wrote:

> The existence of a property right is but one element in determining whether expectations of privacy are legitimate. 'The premise that property interests control the right of the Government to search and seize has been discredited.' *Katz*.

Disharmony with a substantial body of existing case law is only one of the problems with the Court's approach in this case.

I will briefly note four others. First, the Court's reasoning largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation). Attaching such an object is generally regarded as so trivial that it does not provide a basis for recovery under modern tort law. See Prosser & Keeton on Law of Torts (harmless or trivial contact with personal property not actionable). But under the Court's reasoning, this conduct may violate the Fourth Amendment. By contrast, if long-term monitoring can be accomplished without committing a technical trespass—suppose, for example, that the Federal Government

---

[3] The Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience.

required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court's theory would provide no protection.

Second, the Court's approach leads to incongruous results. If the police attach a GPS device to a car and use the device to follow the car for even a brief time, under the Court's theory, the Fourth Amendment applies. But if the police follow the same car for a much longer period using unmarked cars and aerial assistance, this tracking is not subject to any Fourth Amendment constraints.

In the present case, the Fourth Amendment applies, the Court concludes, because the officers installed the GPS device after respondent's wife, to whom the car was registered, turned it over to respondent for his exclusive use. But if the GPS had been attached prior to that time, the Court's theory would lead to a different result. The Court proceeds on the assumption that respondent "had at least the property rights of a bailee," but a bailee may sue for a trespass to chattel only if the injury occurs during the term of the bailment. So if the GPS device had been installed before respondent's wife gave him the keys, respondent would have no claim for trespass—and, presumably, no Fourth Amendment claim either. [Discussion of third problem omitted]

Fourth, the Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked. For example, suppose that the officers in the present case had followed respondent by surreptitiously activating a stolen vehicle detection system that came with the car when it was purchased.

In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap. In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.

Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. See *Knotts*. But the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4–week mark. Other cases may present more difficult questions. But where uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant. We also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy. In such cases, long-term tracking might have been mounted using previously available techniques.

For these reasons, I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment. I therefore agree with the majority that the decision of the Court of Appeals must be affirmed.

Notes

1. Though the history of this trespass-centric approach to the Fourth Amendment has been questioned,[81] it is still the starting point of modern Fourth Amendment analysis. After *Jones*, it is clear that the Court added the *Katz* reasonable-expectation-of-privacy test to the existing trespass framework, creating a new way for non-trespasses to violate the Fourth Amendment. But trespass remains an independently sufficient way to implicate Fourth Amendment protections.
2. If one is in favor of maximal privacy protections, should one join the majority here? Both the majority somewhat snidely, and Sotomayor somewhat more politely, make the point that the *Jones* majority is only adding a new way in which the government might violate the Fourth Amendment. Is that right? If so, why is Alito's concurrence so vociferous?
3. Alito is arguing that the duration of surveillance is highly relevant. Surveys have shown that this is not reflected strongly in public attitudes. A representative sample of Americans was asked whether it would violate a person's expectation of privacy for the government to use their car's onboard GPS system to locate it or track it for a day, a week, or a month. A majority of respondents thought that all of these options would violate an expectation of privacy. Further, over 70% of people gave the same answer (on a five point scale) to the "locate" question as to the "one month" question. Only 5% of respondents showed a rising trend that passed the scale's midpoint – effectively changing from "no" to "yes" on the privacy question.[82]
4. Because of the total of five votes across the two concurrences, the alternative holding that prolonged GPS surveillance violates reasonable expectations of privacy is sometimes called the second majority opinion. You will see Roberts citing it extensively in the later *Carpenter* case.
5. The following year the Court held in *Florida v. Jardines*, 569 U.S. 1 (2013) that bringing a drug-sniffing dog to the porch of a house was a search because "the detectives had all four of their feet and all four of their companion's firmly planted on the constitutionally protected extension of Jardines' home," and had neither express nor implied permission to be there. Though "a police officer not armed with a warrant may approach a home and knock, precisely because that is 'no more than any private citizen might do,' . . . introducing a trained police dog to explore the area around the home in hopes of discovering incriminating evidence is something else." In concurrence, Justice Kagan likened it to a stranger coming up to your windows with high-powered binoculars. But in dissent, Justice Alito (writing for four) disagreed. "The law of trespass generally gives members of the public a license to use a walkway to approach the front door of a house and to remain there for a brief time. This license is not limited to persons who intend to speak to an occupant or who actually do so. According to the Court, however, the police officer in this case committed a trespass because he was accompanied during his otherwise lawful visit to the front door of respondent's house by his dog, Franky. Where is the authority evidencing such a rule? Dogs have been domesticated for about 12,000 years." In effect, a dog sniff is not like a thermal-imaging camera.

---

[81] The trespass-based understanding of the Fourth Amendment has been questioned as a historical matter. *See* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV 67, 67–68 (2013) ("The standard account in Fourth Amendment scholarship teaches that the Supreme Court equated searches with trespasses until the 1960s. [N]o trespass test was used in the pre-*Katz* era. Neither the original understanding nor Supreme Court doctrine equated searches with trespass.").

[82] Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, SUP. Ct. REV. 205, 246–48 (2015).

Jardines emphasizes the difficulty of relying on the law of trespass in a case like this. Girl scouts, vent cleaners, and fundraisers can all regularly be expected to approach a house to hawk their wares. When does doing this constitute a Fourth Amendment search?

From *Jones*, it was clear that it was only a matter of time before the Court was faced with the question of location tracking using purely electronic means. Despite the obviousness of this question, it was not until June 2018 that we received an answer. And, notably, the unanimous result—if split reasoning—of *Jones* completely shattered when the Court was faced with the harder question in *Carpenter*.

Carpenter v. United States, 585 U.S. 296 (2018)

Chief Justice ROBERTS delivered the opinion of the Court.

This case presents the question whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.

I

A

There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people. Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called "cell sites." Although cell sites are usually mounted on a tower, they can also be found on light posts, flagpoles, church steeples, or the sides of buildings. Cell sites typically have several directional antennas that divide the covered area into sectors.

Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas.

Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here. While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.

B

In 2011, police officers arrested four men suspected of robbing a series of Radio Shack and (ironically enough) T–Mobile stores in Detroit. One of the men confessed that, over the previous four months, the group (along with a rotating cast of getaway drivers and lookouts) had robbed nine different stores in Michigan and Ohio. The suspect identified 15 accomplices who had participated in the heists and gave the FBI some of their cell phone numbers; the FBI then reviewed his call records to identify additional numbers that he had called around the time of the robberies.

Based on that information, the prosecutors applied for court orders under the Stored Communications Act to obtain cell phone records for petitioner Timothy Carpenter and several other suspects. That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Federal Magistrate Judges issued two orders directing Carpenter's wireless carriers—MetroPCS and Sprint—to disclose "cell/site sector [information] for [Carpenter's] telephone[ ] at call origination and at call termination for incoming and outgoing calls" during the four-month period when the string of robberies occurred. The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records covering the period when Carpenter's phone was "roaming" in northeastern Ohio. Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day.

Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence. Prior to trial, Carpenter moved to suppress the cell-site data provided by the wireless carriers. He argued that the Government's seizure of the records violated the Fourth Amendment because they had been obtained without a warrant supported by probable cause. The District Court denied the motion.

At trial, seven of Carpenter's confederates pegged him as the leader of the operation. In addition, FBI agent Christopher Hess offered expert testimony about the cell-site data. Hess explained that each time a cell phone taps into the wireless network, the carrier logs a time-stamped record of the cell site and particular sector that were used. With this information, Hess produced maps that placed Carpenter's phone near four of the charged robberies. In the Government's view, the location records clinched the case: They confirmed that Carpenter was "right where the . . . robbery was at the exact time of the robbery." Carpenter was convicted on all but one of the firearm counts and sentenced to more than 100 years in prison. The Court of Appeals for the Sixth Circuit affirmed.

II

A

[Reviewing the Fourth Amendment and *Katz*]

As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to "assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States* (2001). For that reason, we rejected in *Kyllo* a mechanical interpretation of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search. Because any other conclusion would leave homeowners at the mercy of advancing technology, we determined that the Government—absent a warrant—could not capitalize on such new sense-enhancing technology to explore what was happening within the home.

Likewise in *Riley v. California* (2014), the Court recognized the immense storage capacity of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone. We explained that while the general rule allowing warrantless searches incident to arrest strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to the vast store of sensitive information on a cell phone.

B

The case before us involves the Government's acquisition of wireless carrier cell-site records revealing the location of Carpenter's cell phone whenever it made or received calls. This

sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents. Instead, requests for cell-site records lie at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake.

The first set of cases addresses a person's expectation of privacy in his physical location and movements. In *United States v. Jones* (2012), FBI agents installed a GPS tracking device on Jones's vehicle and remotely monitored the vehicle's movements for 28 days. The Court decided the case based on the Government's physical trespass of the vehicle. At the same time, five Justices agreed that related privacy concerns would be raised by, for example, "surreptitiously activating a stolen vehicle detection system" in Jones's car to track Jones himself, or conducting GPS tracking of his cell phone. (ALITO, J., concurring in judgment) (SOTOMAYOR, J., concurring). Since GPS monitoring of a vehicle tracks "every movement" a person makes in that vehicle, the concurring Justices concluded that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"—regardless whether those movements were disclosed to the public at large.

In a second set of decisions, the Court has drawn a line between what a person keeps to himself and what he shares with others. We have previously held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland* (1979). That remains true "even if the information is revealed on the assumption that it will be used only for a limited purpose." *United States v. Miller* (1976). As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections.

This third-party doctrine largely traces its roots to *Miller*. While investigating Miller for tax evasion, the Government subpoenaed his banks, seeking several months of canceled checks, deposit slips, and monthly statements. The Court rejected a Fourth Amendment challenge to the records collection. For one, Miller could "assert neither ownership nor possession" of the documents; they were "business records of the banks." For another, the nature of those records confirmed Miller's limited expectation of privacy, because the checks were "not confidential communications but negotiable instruments to be used in commercial transactions," and the bank statements contained information "exposed to [bank] employees in the ordinary course of business." The Court thus concluded that Miller had "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government."

Three years later, *Smith* applied the same principles in the context of information conveyed to a telephone company. The Court ruled that the Government's use of a pen register—a device that recorded the outgoing phone numbers dialed on a landline telephone—was not a search. Noting the pen register's "limited capabilities," the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial." Telephone subscribers know, after all, that the numbers are used by the telephone company "for a variety of legitimate business purposes," including routing calls. And at any rate, the Court explained, such an expectation "is not one that society is prepared to recognize as reasonable." When Smith placed a call, he "voluntarily conveyed" the dialed numbers to the phone company by "expos[ing] that information to its equipment in the ordinary course of business." Once again, we held that the defendant "assumed the risk" that the company's records "would be divulged to police."

III

The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.

At the same time, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller*. But while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records. After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.

We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search.[3]

A

A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz*. A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. *Jones* (ALITO, J., concurring in judgment) (SOTOMAYOR, J., concurring). Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." *Id.* (ALITO, J., concurring in judgment). For that reason, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."

Allowing government access to cell-site records contravenes that expectation. Although such records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location. Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations." *Jones* (SOTOMAYOR, J., concurring). These location records "hold for many Americans the 'privacies of life.'" And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.

In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*. Unlike the bugged container in *Knotts* or the car in *Jones,* a cell phone—almost a "feature of human anatomy," *Riley*—tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other

[3] The parties suggest as an alternative to their primary submissions that the acquisition of CSLI becomes a search only if it extends beyond a limited period. As part of its argument, the Government treats the seven days of CSLI requested from Sprint as the pertinent period, even though Sprint produced only two days of records. [W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.

potentially revealing locales. Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.

Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when.

Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.

The Government and Justice KENNEDY contend, however, that the collection of CSLI should be permitted because the data is less precise than GPS information. Not to worry, they maintain, because the location records did "not on their own suffice to place [Carpenter] at the crime scene"; they placed him within a wedge-shaped sector ranging from one-eighth to four square miles. Yet the Court has already rejected the proposition that "inference insulates a search." *Kyllo*. From the 127 days of location data it received, the Government could, in combination with other information, deduce a detailed log of Carpenter's movements, including when he was at the site of the robberies. And the Government thought the CSLI accurate enough to highlight it during the closing argument of his trial.

At any rate, the rule the Court adopts "must take account of more sophisticated systems that are already in use or in development." *Kyllo*. While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision. As the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas. In addition, with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters.

Accordingly, when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.

B

The Government's primary contention to the contrary is that the third-party doctrine governs this case. In its view, cell-site records are fair game because they are "business records" created and maintained by the wireless carriers. The Government (along with Justice KENNEDY) recognizes that this case features new technology, but asserts that the legal question nonetheless turns on a garden-variety request for information from a third-party witness.

The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government

thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.

The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of "diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." *Smith* and *Miller*, after all, did not rely solely on the act of sharing. Instead, they considered "the nature of the particular documents sought" to determine whether "there is a legitimate 'expectation of privacy' concerning their contents." *Smith* pointed out the limited capabilities of a pen register; as explained in *Riley*, telephone call logs reveal little in the way of "identifying information." *Miller* likewise noted that checks were "not confidential communications but negotiable instruments to be used in commercial transactions." In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.

The Court has in fact already shown special solicitude for location information in the third-party context. In *Knotts*, the Court relied on *Smith* to hold that an individual has no reasonable expectation of privacy in public movements that he "voluntarily conveyed to anyone who wanted to look." But when confronted with more pervasive tracking, five Justices agreed that longer term GPS monitoring of even a vehicle traveling on public streets constitutes a search. *Jones*. Justice GORSUCH wonders why "someone's location when using a phone" is sensitive, and Justice KENNEDY assumes that a person's discrete movements "are not particularly private." Yet this case . . . is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*.

Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly "shared" as one normally understands the term. In the first place, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. *Riley*. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[ ] the risk" of turning over a comprehensive dossier of his physical movements. *Smith*.

We therefore decline to extend *Smith* and *Miller* to the collection of CSLI. Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection. The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.

Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security. As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not "embarrass the future." *Northwest Airlines, Inc. v. Minnesota* (1944).

As Justice Brandeis explained in his famous dissent, the Court is obligated—as "[s]ubtler and more far-reaching means of invading privacy have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections. *Olmstead v. United States* (1928). Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers, "after consulting the lessons of history," drafted the Fourth Amendment to prevent.

We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment.

Justice KENNEDY, with whom Justice THOMAS and Justice ALITO join, dissenting.

This case involves new technology, but the Court's stark departure from relevant Fourth Amendment precedents and principles is, in my submission, unnecessary and incorrect, requiring this respectful dissent.

The new rule the Court seems to formulate puts needed, reasonable, accepted, lawful, and congressionally authorized criminal investigations at serious risk in serious cases, often when law enforcement seeks to prevent the threat of violent crimes. And it places undue restrictions on the lawful and necessary enforcement powers exercised not only by the Federal Government, but also by law enforcement in every State and locality throughout the Nation. Adherence to this Court's longstanding precedents and analytic framework would have been the proper and prudent way to resolve this case.

The Court has twice held that individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party. *United States v. Miller* (1976); *Smith v. Maryland* (1979). This is true even when the records contain personal and sensitive information. So when the Government uses a subpoena to obtain, for example, bank records, telephone records, and credit card statements from the businesses that create and keep these records, the Government does not engage in a search of the business's customers within the meaning of the Fourth Amendment.

In this case petitioner challenges the Government's right to use compulsory process to obtain a now-common kind of business record: cell-site records held by cell phone service providers. Petitioner acknowledges that the Government may obtain a wide variety of business records using compulsory process, and he does not ask the Court to revisit its precedents. Yet he argues that, under those same precedents, the Government searched his records when it used court-approved compulsory process to obtain the cell-site information at issue here.

Cell-site records, however, are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process. Customers like petitioner do not own, possess, control, or use the records, and for that reason have no reasonable expectation that they cannot be disclosed pursuant to lawful compulsory process.

The Court today disagrees. It holds for the first time that by using compulsory process to obtain records of a business entity, the Government has not just engaged in an impermissible action, but has conducted a search of the business's customer. The Court further concludes that the search in this case was unreasonable and the Government needed to get a warrant to obtain more than six days of cell-site records.

In concluding that the Government engaged in a search, the Court unhinges Fourth Amendment doctrine from the property-based concepts that have long grounded the analytic

framework that pertains in these cases. In doing so it draws an unprincipled and unworkable line between cell-site records on the one hand and financial and telephonic records on the other. According to today's majority opinion, the Government can acquire a record of every credit card purchase and phone call a person makes over months or years without upsetting a legitimate expectation of privacy. But, in the Court's view, the Government crosses a constitutional line when it obtains a court's approval to issue a subpoena for more than six days of cell-site records. That distinction is illogical and will frustrate principled application of the Fourth Amendment in many routine yet vital law enforcement operations.

The Court appears, in my respectful view, to read *Miller* and *Smith* to establish a balancing test. For each "qualitatively different category" of information, the Court suggests, the privacy interests at stake must be weighed against the fact that the information has been disclosed to a third party. When the privacy interests are weighty enough to "overcome" the third-party disclosure, the Fourth Amendment's protections apply.

That is an untenable reading of *Miller* and *Smith*. As already discussed, the fact that information was relinquished to a third party was the entire basis for concluding that the defendants in those cases lacked a reasonable expectation of privacy. *Miller* and *Smith* do not establish the kind of category-by-category balancing the Court today prescribes.

Justice GORSUCH, dissenting.

In the late 1960s this Court suggested for the first time that a search triggering the Fourth Amendment occurs when the government violates an "expectation of privacy" that "society is prepared to recognize as 'reasonable.'" *Katz v. United States* (1967) (Harlan, J., concurring). Then, in a pair of decisions in the 1970s applying the *Katz* test, the Court held that a "reasonable expectation of privacy" *doesn't* attach to information shared with "third parties." By these steps, the Court came to conclude, the Constitution does nothing to limit investigators from searching records you've entrusted to your bank, accountant, and maybe even your doctor.

What's left of the Fourth Amendment? Today we use the Internet to do most everything. Smartphones make it easy to keep a calendar, correspond with friends, make calls, conduct banking, and even watch the game. Countless Internet companies maintain records about us and, increasingly, *for* us. Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did.

Today the Court suggests that *Smith* and *Miller* distinguish between *kinds* of information disclosed to third parties and require courts to decide whether to "extend" those decisions to particular classes of information, depending on their sensitivity. But . . . no balancing test of this kind can be found in *Smith* and *Miller*. Those cases announced a categorical rule: Once you disclose information to third parties, you forfeit any reasonable expectation of privacy you might have had in it.

The problem isn't with the Sixth Circuit's application of *Smith* and *Miller* but with the cases themselves. Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can—at least without running afoul of *Katz*. But that result strikes most lawyers and judges today—me included—as pretty unlikely.

What does all this mean for the case before us? To start, I cannot fault the Sixth Circuit for holding that *Smith* and *Miller* extinguish any *Katz*-based Fourth Amendment interest in third party cell-site data. That is the plain effect of their categorical holdings. Nor can I fault the Court today for its implicit but unmistakable conclusion that the rationale of *Smith* and *Miller* is wrong; indeed, I agree with that. The Sixth Circuit was powerless to say so, but this

Court can and should. At the same time, I do not agree with the Court's decision today to keep *Smith* and *Miller* on life support and supplement them with a new and multilayered inquiry that seems to be only *Katz*-squared.

Our case offers a cautionary example. It seems to me entirely possible a person's cell-site data could qualify as *his* papers or effects under existing law. Yes, the telephone carrier holds the information. But 47 U.S.C. § 222 designates a customer's cell-site location information as "customer proprietary network information" (CPNI), and gives customers certain rights to control use of and access to CPNI about themselves. Those interests might even rise to the level of a property right.

The problem is that we do not know anything more. Before the district court and court of appeals, Mr. Carpenter pursued only a *Katz* "reasonable expectations" argument. He did not invoke the law of property or any analogies to the common law, either there or in his petition for certiorari. Even in his merits brief before this Court, Mr. Carpenter's discussion of his positive law rights in cell-site data was cursory. He offered no analysis, for example, of what rights state law might provide him in addition to those supplied by § 222. In these circumstances, I cannot help but conclude—reluctantly—that Mr. Carpenter forfeited perhaps his most promising line of argument.

Notes

1. In *Carpenter*, Roberts is making two major moves in his efforts to reform the third-party doctrine. First, he is saying that the third-party doctrine is not absolute. The Fourth Amendment protects some information shared with third parties. Second, he is saying that cellphone location data is special—at least when compared to bank and call record data. The dissent questions both of these conclusions. Is Roberts right to privilege location data over financial data? How much can you tell about a person by combining their credit card, bank, and Venmo histories? One could easily argue that the changing role of credit cards has made them as essential to life as cellphones, and that the breadth of their use makes them as revealing as location data.[83]
2. What exactly is the *Carpenter* test? Several factors appear to be critical to the decision: that the cellphone is indispensable to modern life and therefore its use is effectively nonvoluntary; that location monitoring is inescapable if one uses a cellphone; and that the information gathered by such nonvoluntary and inescapable surveillance is uniquely intrusive. Matthew Tokson conducted an empirical review of lower court post-*Carpenter* cases and found a number of patterns.[84] First, courts were more likely to extend *Carpenter* to cover cases that included digital than non-digital data (finding a search in 35.8% of cases and 15.5% of cases, respectively). Overall, courts most frequently considered:

> "[T]he revealing nature of the data collected; the amount of data collected; and the automatic nature of disclosure to third parties clearly and powerfully influence case outcomes in post-*Carpenter* law. The number of persons affected has little or no influence on case outcomes, and indeed has been overtly rejected by some courts. The remaining factors of inescapability and cost are influential when they appear but are rarely discussed by courts in the dataset; their importance going forward is ambiguous."

---

[83] *See, e.g.*, Matthew B. Kugler & Meredith Hurley, *Protecting Energy Privacy Across the Public/Private Divide*, 72 FLA. L. REV. 451, 487 (2020) (noting that in the time of *Miller* only about sixteen percent of families had a bank-type credit card but now the overwhelming majority of purchases are done using credit or debit cards).

[84] Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 HARV. L. REV. 1790 (2022).

3. Though the third-party doctrine has appeared rarely at the Supreme Court since the 1970s, it has been used widely by lower courts. In the pre-*Carpenter* case *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008), the Ninth Circuit reasoned that IP addresses are just the Internet equivalent of numbers dialed. Is that still the right answer, or is a list of the websites a person has visited "*Carpenter*-like" data? When presented with materially indistinguishable facts post-*Carpenter* in *United States v. Soybel,* 13 F.4th 584, 592 (7th Cir. 2021), the Seventh Circuit held it was not a search for the government to obtain the IP addresses of all websites, external connections, and timestamps that a computer account had made through use of a pen register. It argued that the "unique features of historical CSLI are absent for IP-address data" so "this case bears the hallmarks of *Smith* not *Carpenter*."
4. Similarly, one could question whether previous cases about utility records are still valid given the rise of smart meters, which can record electricity consumption in minute-by-minute intervals.[85] In *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 527–28 (7th Cir. 2018), the Seventh Circuit found an expectation of privacy in smart meter data under *Carpenter*. It then held that mandatory installation of such meters was a reasonable regulatory search provided that such data would not be used for law enforcement purposes without a warrant.
5. The extent to which one can push *Carpenter* to overturn previous anti-privacy Fourth Amendment holdings has been examined in pretty much every major search domain. This includes facial recognition, tower dumps (getting a list of phones near a cell tower at a particular time), and automated license plate readers.[86]

Chatrie v. United States, 609 U.S. ___ (2026)

Justice Kagan delivered the opinion of the Court.

Modern cell phones…are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley* v. *California* (2014). Since then, the percentage of Americans who own smartphones has only increased. Today, more than nine in ten Americans own a smartphone. That means they are likely addicted to apps and other services, many of which collect and store "detailed information about all aspects of a person's life." *Riley*.

Among that information is a single fact most pertinent here: where the user's cell phone is located at a given time. Apps of many kinds rely on that datum. Your maps app wants to help you navigate from Point A (where you are) to Point B (where you are going). Ride-sharing apps of course track your location when you are using them, and often do so even when you are not. Weather apps want to tell you about local conditions. Fast-food apps want to identify the closest burger and pizza joints. Fitness apps want to track your running routes. And so on.

This case concerns a form of cell-phone location data called "Location History," which Google apps collect and store.[1] Location History is what it sounds like—a time-stamped record of every place a cell phone has been. Every two minutes or so, Location History draws from an array of sources to log a cell phone's location. Those sources include nearby Wi-Fi networks, Bluetooth beacons, and cell sites, as well as GPS and IP address information. When combined,

---

[85] For a discussion of this issue, see Matthew B. Kugler & Meredith Hurley, *Protecting Energy Privacy Across the Public/Private Divide*, 72 FLA. L. REV. 451 (2020).

[86] *See, e.g.*, Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105 (2021); Emma Lux, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AMER. CRIM. L. REV. 109 (2020).

[1] Throughout this opinion, we describe how Location History worked at the time the warrant at issue was executed. As noted below, Google has since then instituted a significant change, which apparently insulates Location History data from geofence warrants

the signals tracked can determine a cell phone's location within 20 meters. They can also ascertain a phone's elevation, and thus reveal which floor within a building the phone is on. By all accounts, those features make Location History "the most sweeping, granular, and comprehensive tool" existing today for collecting and storing location data.

Google repeatedly prompts users to enable Location History, and over 500 million users worldwide have done so. The first prompt comes when a user initially establishes a Google account. If that spur is ignored, another will arrive when a user sets up a Google app—like Google Assistant, Google Maps, or Google Photos—on his phone or other device. Android (though not iPhone) users are specifically warned that their devices will not "work correctly" unless they turn on Location History. And once a user does so, the service runs—and runs constantly—in the background. Regardless whether the user has a Google app open—or whether he is using his phone at all—Location History remains active. Indeed, it continues to work even if the user deletes the app through which he first turned it on. Location History stops only if a user affirmatively stops it. Sans that intervention, it tracks and tracks and tracks a user's cell phone (and other devices).

Google stores all Location History data in the cloud, rather than on a user's device—though that choice makes no real difference to the user. "Cloud computing" refers to "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." Because it exists, Google can store information on its own servers, while the user can view it as if stored on his cell phone. Such remote storage, we have explained, is common: "Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference." So, for example, Google usually stores users' emails, documents, and photographs on company servers instead of on individual devices. And the same is true of the information generated by Location History, which is stored in a single central repository on Google's servers.[2] That data exists someplace remote, but a user sees it—and the content Google creates from it—in the palm of his hand. The user thus can access a "Timeline" showing where he has traveled when; receive real-time updates about his daily commute; and take advantage of maps and recommendations based on his usual movements.

In the last decade, Google's Location History data has also served another function, though this one unknown to most users: That data, as obtained through a geofence warrant, can enable law enforcement officers to solve hard-to-solve crimes. Such a warrant, as earlier described, seeks information about the cell phones located in the vicinity of a crime scene at around the time the crime was committed. The goal, put simply, is to find out who was there and so who might have done it. (There are usually better ways to investigate an already-known suspect—like seeking only his location data.) And the mechanism is to use the offender's cell phone as an identifying device. The warrant specifies a timeframe and maps an area (with the geofence as its perimeter), and demands information about the cell phones—and their users—present within it. There is some uncertainty about how often the technique in fact works. But its use among law enforcement officers has flourished. Google received its first geofence warrant in 2016. Two years later, it received 982; and two years after that, more than 11,000. Though the details vary, each has made the same essential demand: Tell us, through cell-phone location data, who was there when a crime happened.[3]

---

[2] Except that in July 2025, years after the geofence warrant used in this case, Google made a change: It now stores Location History data on individual users' devices rather than on its own servers. Google represents that, as a result, it is no longer capable of responding to geofence warrants that seek Location History data.

[3] Google is not the only tech company that has received geofence warrants; so have Apple, Lyft, Snapchat, and Uber, among others. But Google is the "most common recipient and the only one known to respond."

As those demands began to proliferate, Google worked with law enforcement officials to develop a three-step protocol to govern geofence warrants. At the first step, Google produces anonymized (*i.e.*, no names attached) location data for all cell phones (or other devices) within the geofence—typically, a circle with a designated radius surrounding a latitude/longitude coordinate—during a specified timeframe. That data generally includes each phone's latitude/longitude coordinate and corresponding timestamp; an estimate of that information's accuracy; and a description of the information's source (*e.g.*, a Wi-Fi network, a cell site, or some other). The data at this stage shows each user's location, every two minutes or so, within the geofence. At the second step of the process, officials review the data produced and typically ask Google to provide additional information for a subset of still-anonymized users. That new data is usually for a longer timeframe than first specified; it also shows the user's location outside, as well as inside, the geofence. Finally, at the third step, officials demand the identities of a further subset of users—their names, email addresses, and phone numbers. Thus, the geofence warrant is designed to eventually produce a select number of identified users suspected of committing the crime under investigation.

On May 20, 2019, at about 4:50 p.m., a man robbed a credit union in Midlothian, Virginia. The robber presented a teller with a handwritten note demanding $100,000, threatening to hurt her and her family if she did not comply, and warning her that he had "boys on the lookout out side." When the teller replied that she did not have access to that amount of money, the robber brandished a firearm. He ordered everyone in the bank to the ground, and forced the bank's manager to open a safe and put $195,000 into a bag. The robber then left on foot with the money.

Local police officers responded to the scene and began an investigation. They learned, from witness interviews and surveillance-camera footage, that the robber had approached the credit union from a corner of an adjacent church, while appearing to talk on a cell phone. But they could not find out anything more, and the robber remained at large.

On June 14, the police officers thus applied to a Virginia magistrate for a geofence warrant directed to Google. The application described the cell-phone location data Google collects, and explained how that data could lead to identifying the robber, his possible accomplices, or additional witnesses to the crime. Success was particularly likely here, the application stated, because the robber appeared to be using his phone when he entered the credit union, and may even have been speaking with an accomplice. The officers' proposed geofence was a circle with a radius of 150 meters surrounding the credit union.

The magistrate issued the warrant, and officers executed it in the manner prescribed. At the first stage of the process, Google gave up anonymized data for 19 users found within the geofence during the hour within which the robbery occurred. At the second stage, the officers winnowed the list to nine users. And Google produced anonymized data showing their movements both inside and outside the geofence for the extended two-hour period. At the third and last step, the police again narrowed the list, this time to three users. Google responded with their identifying information. One of the three was Chatrie. The location data showed that he entered the geofenced area about ten minutes before the robbery, and headed toward a residential area of town immediately after leaving the bank.

Following further police work, a federal grand jury charged Chatrie with robbery…

We granted certiorari solely on the question whether the police violated the Fourth Amendment in obtaining Chatrie's location data, thus declining to consider the exclusionary rule issue. The disputed Fourth Amendment question divides into two parts. First, did law enforcement officials conduct a search under the Fourth Amendment when they acquired Chatrie's location data from Google? We hold that they did because an individual has a legitimate expectation of privacy in his cell-phone location data. Second, did the multi-step geofence warrant issued here make that search reasonable? We leave that question—which

requires deciding whether the warrant satisfied the Fourth Amendment's probable cause and particularity requirements at each stage of the search process—to the Court of Appeals to address in the first instance.[4]

II

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The "basic purpose" of that Amendment, our precedents say, is "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Carpenter* v. *United States* (2018).

…Whether an expectation of privacy counts as legitimate is less the result of any fixed set of rules than of "guideposts" stretching back to the Fourth Amendment's beginnings. From the founding onward, we have explained, the Fourth Amendment has sought to secure the "privacies of life" against the exercise of "arbitrary power." So too we have recognized, and repeatedly, that the Amendment was designed "to place obstacles in the way of a too permeating police surveillance." Whatever the form of an attempted incursion, the Fourth Amendment protects Americans' long-held conviction that no government official should have free access to the most closely kept aspects of their lives.

In recent decades, this Court has often confronted the challenge of adhering to those principles in the face of new technologies. "[I]nnovations in surveillance tools" have "enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes." The Court, in response, has sought to "assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo* v. *United States* (2001).

We begin with *Carpenter* in considering the Government's front-line position here: that no warrant was needed to get Location History data from Google (although the police "prophylactically secured" one) because no Fourth Amendment search ever took place. We then explain why the result we reached in *Carpenter* once again follows. Contrary to the Government's view, an individual has a legitimate expectation of privacy in the information Location History collects about his cell phone's—meaning his own—movements. The police invade that expectation, and thus conduct a search, when they acquire that information, even though for only a limited period of time and even though via a third-party tech company.

The question presented in *Carpenter* was "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." The cell-phone records at issue were what is known as cell-site location information (CSLI). As we explained, CSLI is a "time-stamped record" generated each time a cell phone connects to a cell site. Wireless carriers collect and store that information for their own business purposes (such as finding weak spots in their networks). But CSLI can also benefit law enforcement, because it identifies an individual's approximate location every time his phone makes a connection. In *Carpenter*, police officers investigating a string of Radio Shack robberies ordered a wireless carrier of a known suspect to turn over his CSLI records for a seven-day period (without first getting a warrant). Those records showed, as the Government later put it, that the suspect, Timothy Carpenter, was "right where the ... robbery was at the exact time of the robbery." Carpenter moved to exclude the CSLI records, arguing that the Government acquired them through an unconstitutional search.

The resemblances between CSLI and Location History, in their relationship to personal privacy, practically leap off the page. Everything *Carpenter* relied on to find that law

[4] In line with our grant of certiorari, we do not address whether the good-faith exception to the exclusionary rule still allows the admission of the Location History data in this case. That question remains for the Fourth Circuit to consider anew, gleaning anything it thinks relevant from our decision on the substantive Fourth Amendment issues.

enforcement officers conducted a Fourth Amendment search when they accessed wireless carriers' CSLI records applies as well or better to the police's accessing of Google's Location History data.

First, Location History provides an even more fine-tuned picture of a person's movements than CSLI. *Carpenter* noted that through CSLI records, police could "achieve[ ] near perfect surveillance" of an individual holding a cell phone. But Location History is nearer perfect still. Here is one way of comparing the two: At any given time, CSLI placed Carpenter within a "sector ranging from one-eighth to four square miles," whereas Location History pinpointed Chatrie's location within around twenty meters, which is less than two percent of a mile. Or here is another measure: CSLI logged Carpenter's location an average of 101 times a day, whereas Location History commonly records a person's location every two minutes, for a daily average of 720 chartings. Or finally, a third: Unlike CSLI, Location History can estimate a phone's elevation—so, for example, can tell whether someone has gone into a doctor's office on the first floor of a multi-story building, or a private apartment on the tenth. …[A]cross the board Location History is the far more precise measure. When the *Carpenter* Court said that CSLI provides a "detailed" and "encyclopedic" portrait of a person's whereabouts, it did not know what further technology was on the horizon.

And next, Location History also allows police officers to reconstruct "retrospective[ly]," and with no real effort, people's comings and goings in any area. As with CSLI, the Government need not decide in advance the kind of surveillance it should undertake, whether of a person or a site….

Indeed, Location History records implicate those privacy interests still more than CSLI data because the former is more the individual's own. …Google users, too, regularly employ Location History—for example, "to remind themselves of a restaurant they ate at two weeks ago, the time they were last at a friend's home, the sites they saw on vacation, or the distance they walked on a particular day." The records thus serve as a personal journal of a user's movements, which that user consults (and even can edit) for his own purposes. In that way, Location History resembles other private materials—think of emails, documents, photographs, or calendars—that even if stored on Google's servers, a user reasonably views as his own. And as a result, that he reasonably expects to be shielded from the "inquisitive eyes" of the government.

The Government, not much contesting any of the above, principally argues on a different ground: that accessing only a short amount of cell-phone location information (whether Location History or CSLI) does not count as a Fourth Amendment search. Recall that *Carpenter* involved seven days' worth of location data. And in deciding that case, this Court reserved the issue whether there was a more "limited period for which the Government may obtain" such data "free from Fourth Amendment scrutiny." The Government now claims that the answer is yes, and that the two hours' worth of Location History acquired here falls within the Constitution-free zone. In the Government's view, a person has no reasonable expectation of privacy in "that short a time window" of location data, because his "short-term" movements will "reveal[ ] little about the details of [his] personal life."

But to begin, the Government is wrong about the incapacity of short-term location information to reveal private matters. Return here to another of *Jones*'s insights: "[E]ven short-term monitoring" of a person's physical movements can provide "a wealth of detail about [his] familial, political, professional, religious, and sexual associations." (opinion of Sotomayor, J.). Consider just a few trips that a person is apt to think "indisputably private": to "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, [or] the by-the-hour motel." Location History—even two hours of it—allows officers to target one-off events of potential interest: a gun show, say, or a political rally.

Still more fundamentally, we have never understood Fourth Amendment protections as kicking in only once an intrusion "goes too far." *Pennsylvania Coal Co.* v. *Mahon* (1922) (adopting that approach for regulatory takings). Where the Fourth Amendment applies, it applies—regardless of "the quality or quantity of information" the government obtains. *Kyllo*. So, for example, this Court held that thermal imaging qualified as a search even though it did not, and was not likely to, detect "private activities" or "intimate details." The Amendment, we analogized, makes "no exception" for the officer "who barely cracks open the front door and sees nothing but the nonintimate rug on the vestibule floor."

That approach makes all the more sense when, as with Location History, officials can select the time-limited set of materials they want from an all-encompassing database. Then, the durational bounds on the data actually acquired do little to address the Fourth Amendment's concern about "a too permeating police surveillance." *Di Re*. What creates that concern is that the government can access all of a cell-phone user's movements, in both public and private places—that it possesses a virtual panopticon with which to scrutinize its citizens' activities.

The Government has an additional argument, which in *Carpenter* was its "primary" one—that the so-called third-party doctrine precludes Chatrie from invoking the Fourth Amendment's protections. The idea is that in "authoriz[ing] Google to collect, retain, and use" his location information, Chatrie lost his legitimate expectation of privacy. The problem for the Government is that *Carpenter* refused to apply the third-party doctrine to CSLI, and no good reason exists to reach a different result for Location History.

In *Carpenter*, the Court rejected the Government's contention that the third-party doctrine likewise governed the acquisition of CSLI. The Court acknowledged that a cell-phone user "continuously reveals his location" to a third-party wireless carrier. But it held that cell-phone location information is "qualitatively different" from "telephone numbers and bank records." Those differences fell along two axes. First, the Court explained, the "nature" of CSLI is incomparably "revealing." And second, the Court continued, "[c]ell phone location information is not truly 'shared' as one normally understands the term." Because "cell phones and the services they provide" are "such a pervasive and insistent part of daily life"—"indispensable to participation in modern society"—a person can hardly help but generate a "trail of location data." "[I]n no meaningful sense," the Court thought, does that mean a person "voluntar[il]y expos[es]" to any third party a "comprehensive dossier of his physical movements." Both differentiating features highlighted in *Carpenter* apply equally or better to Location History.

The Government contests that conclusion on *Carpenter*'s second axis alone: It claims that generating Location History, unlike producing CSLI, is a voluntary choice on the user's part. Although carrying a cell phone may be indispensable in modern society, the Government argues, using Location History is not. Rather, Location History is an "optional add-on," which a user must enable by an "affirmative act" beyond "powering up" a phone. (quoting *Carpenter*). In support, the Government emphasizes that only around one-third of current Google accountholders have activated the service.

But as an initial matter, that argument ignores some pertinent facts about how and why Google users turn on Location History. As described earlier, Google prompts a user, and repeatedly, to turn on the service—when he sets up a Google account, when he sets up an Android phone, and when he sets up a Google app. The prompt often informs him that his device will not "work correctly" unless he does so. By contrast, it does not tell him quite what he is signing up for: "how frequently Google would record [his] location"; "how precise Location History can be"; or how Google might give all that minute-by-minute location information to the government. In those circumstances, it is hard to see how any user is, in the normal sense, "sharing" with third parties a comprehensive catalog of his physical movements. And that is so regardless of how many others ignore Google's entreaties. … in any event, the raw user totals for Location History—one-third, two-thirds, or someplace in between—are not the most apt

measure of whether that service's enlistees have, as the Government claims, self-consciously "assumed the risk of sharing" all their movements with others.

More generally, the Government's approach to Fourth Amendment protection would raise a host of workability issues. At the top of the list: What percentage of users would have to sign up for a service to make doing so non-voluntary? And after that, the questions only multiply. Would a user lose Fourth Amendment protection if a highly popular cell-phone feature became less so over time? What if the use of a given feature is ubiquitous among (but only among) a subset of the population (say, an age cohort), and an individual defendant is a member of that class? Would it be enough if the lion's share of cell-phone users enabled a feature similar to the one at issue—so, for example, any location-tracking service, whether Google's or some other company's? And finally, a more basic inquiry: In such a world, how is anyone—whether a cell-phone user or a police officer—to know in advance (which is when the knowledge is useful) whether enrollees in a given service will be found to have Fourth Amendment protection in the information that service collects? To ask all these questions about the Government's approach is to know that it is on the wrong track.

And there is yet a deeper problem: The Government's app-by-app, feature-by-feature method of granting Fourth Amendment protection misapprehends the very nature of modern cell-phone use. Pretty much everything a person does on a smartphone requires some kind of opt-in—an "affirmative act" beyond "powering up" to utilize a given app or service. Consider sending an email on Gmail, uploading a photo to Google Photos, or adding a calendar entry to Google Calendar. None happens solely by dint of the phone's operation; each requires, as Location History does, an "optional add-on." And each activity, like using Location History, results in sharing information with a third-party tech company—turning over private materials to live on that company's servers. The Government wishes to disconnect all those uses from the mere act of carrying a turned-on cell phone (the thing that generates CSLI), with only the latter receiving assured Fourth Amendment protection. But that is to imagine that all of us are living in dumb flip-phone days. The point of carrying smartphones is to use what is on them—as *Carpenter* said, to use the apps and "services they provide." *That* is what has become a "pervasive and insistent"—even "indispensable"—"part of daily life." And so *that* is what *Carpenter* insulated from the third-party doctrine. A cell-phone user is not to be viewed as sharing private information with third parties—which then can be freely passed on to the government—just by doing the ordinary things cell-phone users do.

For all those reasons, we hold that police officers invade a cell-phone user's reasonable expectation of privacy when they access his Location History. It does not matter if the time period scrutinized was only two hours. Nor does it matter that the materials obtained were handed over by a third-party tech company. When the government "accesses historical cell phone" location information—Location History as much as CSLI—it "conducts a search under the Fourth Amendment." *Carpenter*.

III

That conclusion does not resolve this case, because the Fourth Amendment prohibits only searches that are "unreasonable." When law enforcement officials undertake a search to discover evidence of a crime, the reasonableness standard generally requires that they seek a warrant from "a neutral and detached magistrate." The magistrate, in turn, may issue a warrant only when "probable cause is properly established and the scope of the authorized search is set out with particularity."

When officers have obtained a warrant, as they did here, a search's legality will thus depend on whether a magistrate has properly found probable cause to support a particularly described search. "[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Illinois* v. *Gates* (1983). But a magistrate must always determine that there is a

"fair probability that contraband or evidence of a crime will be found" in the place searched. That means determining, to the requisite "fair probability," both that the place searched will have the materials sought and that those materials will contain evidence "aid[ing]" in a criminal's "apprehension or conviction." *Messerschmidt* v. *Millender* (2012). The particularity requirement, for its part, ensures that the search will be of an appropriate scope—that it is "carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland* v. *Garrison* (1987). That requirement typically looks to such matters as the geographic and durational expanse of the search. And it too must take account of "particular factual contexts," including in surveillance cases the nature of the technology to be used. *Gates*.

The warrant issued here, as described earlier, was an uncommon, multi-step one. …The parties have contested the legality of each stage of that process. Chatrie analogizes the first step to an "unconstitutional general warrant," and argues that in any event the search at that step was both insufficiently described by the warrant and lacking in probable cause. As to steps two and three, Chatrie contends that the warrant left too much authority to police officers—and too little to the magistrate—to define the search's scope and determine whether cause for it existed. The Government, for its part, defends the warrant at every step as seeking "particularized information from Google's database" based on "probable cause to believe that Google had information" that would help solve a crime. And the Government urges that the discretion given to the officers at steps two and three fell within the bounds of reasonableness.

We leave all of those questions to the Court of Appeals to decide in the first instance. Because the Fourth Circuit panel concluded that no search had occurred, it did not address whether the geofence warrant issued here validly authorized each stage of the search process. We are, as we have said many times before, "a court of review, not of first view.". It is therefore now up to the Court of Appeals to decide whether, at each step of the search process, the warrant satisfied the Fourth Amendment's requirements of particularity and probable cause.

Justice Jackson, with whom Justice Sotomayor joins, concurring.

I agree with the Court that law enforcement officers conducted a search when they accessed petitioner Chatrie's Location History. I write separately because I would have gone further to explain that this search violated the Fourth Amendment. As the Court observes, "[w]hen officers have obtained a warrant," the validity of a search turns on "whether a magistrate has properly found probable cause to support a particularly described search." In my view, it is clear that at a minimum the second and third stages of the search process here did not satisfy this foundational requirement.

At step two, the warrant authorized officers to access an additional hour's worth of Location History, unbounded by the geofence's perimeter. Though the warrant stated that officers would "*attempt* to narrow down the list" of devices subject to this step, there was no explicit requirement that they do so. Nor did the warrant set forth any criteria that officers would use in their narrowing efforts.

The same infirmities carried over to step three. At this step, the warrant authorized officers to access "identifying account information," including the username, date of birth, account number, and any email addresses or telephone numbers associated with the account. Once again, the warrant stated only that officers would "*attempt* to narrow down the list," without setting forth any criteria for doing so.

This "uncommon, multi-step" process meant that officers conducted key portions of the search outside the supervision of "a neutral and detached magistrate," *Johnson* v. *United States*, (1948). Put differently, officers could obtain additional, sensitive information at steps two and three without having to convince a magistrate that there was probable cause to believe this particular information would uncover evidence related to the crime. In this way, the

warrant left "too much to the discretion of the officer[s] executing the order," giving them a "roving commission" to collect more data absent any justification to a magistrate.

The facts of this case illustrate why the lack of magisterial oversight is dangerous. When executing steps two and three, law enforcement initially sought unbounded data and account information from *all* 19 devices identified at step one. Nothing in the warrant prevented officers from obtaining this broad set of data; they narrowed the list only because Google insisted on it…

Justice Gorsuch, concurring in the judgment.

To decide whether a Fourth Amendment search took place in this case, the Court once again invokes a test first advanced in a solo concurrence in *Katz* v. *United States* (1967). Under that test, a search occurs when the government intrudes on an "expectation of privacy" that "society is prepared to recognize as 'reasonable.' "

If *Katz* has become a familiar feature of our law, it seems to me no more persuasive for it. Consider just a few of its problems, beginning with this: It has no basis in the Constitution's text or history. The Fourth Amendment's protections do not depend on "the breach of some abstract 'expectation of privacy' whose contours are left to the judicial imagination." *Carpenter* (Gorsuch, J., dissenting). Instead, the Fourth Amendment speaks in more concrete terms, protecting an individual's person, house, papers, and effects from unreasonable searches and seizures.

Even if I could overlook that problem with *Katz*, I still wouldn't know how to apply it. As the Court has candidly admitted, it has never been able to identify a "single rubric" that might "definitively resolv[e] which expectations of privacy are entitled to protection." *Carpenter*. Maybe *Katz* poses an empirical question, tagging reasonable expectations of privacy to those privacy expectations "people *actually* have." *Carpenter* (Gorsuch, J., dissenting). Or maybe the question is a normative one, asking what expectations reasonable people "*should* ... have." In truth, nobody knows and, either way, this Court is the wrong body for the task. We aren't equipped to make empirical assessments about what most Americans think. Nor is it our job to enforce our own normative judgments, as opposed to those embodied in the Constitution and laws..

If this weren't trouble enough, we've also adorned *Katz* with an equally indefensible qualification called the third party doctrine. …Much as with *Katz* itself, this Court has never offered a persuasive justification for its offshoot. Nor do I see how it might. Do we seriously mean to suggest that most Americans think they have no "reasonable expectation of privacy" in records held for them by their banks or pharmacists or doctors or technology companies? If not, on what authority might we rule that the American people should not reasonably expect privacy in materials like those? Really, the third party doctrine amounts to little more than a "doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants."

As it did eight years ago in *Carpenter*, the Court today largely ignores these problems…Count me unpersuaded. Why does tracking Mr. Chatrie's movements digitally over an hour or two invade his reasonable expectation of privacy when an officer tailing him for the same length of time would not? See *United States* v. *Knotts* (1983). Why is Location History data Mr. Chatrie voluntarily shared with Google not "truly shared" when a person's bank records are? See *Miller*. Does the Court just mean to give *Katz*'s third party doctrine a quiet burial by suggesting today that any information shared over "smartphones" using "apps and services" falls outside its reach?

Rather than employ *Katz* and its third party doctrine, I would take a different approach. To decide whether the Fourth Amendment is in play, I would consult its terms, asking first

whether Location History qualifies as one of Mr. Chatrie's papers or effects, and then asking whether the government searched those papers or effects.

Based on the evidence the parties have put before us, it appears the word "effects" was understood at the time of the Fourth Amendment's adoption to embrace most any kind of personal property

As I see it, Mr. Chatrie's Location History data qualifies as his personal property. To appreciate why, start with this. As Google puts it, and no one seriously disputes, Location History serves as a "diary" or map "of a person's travels." At the time of the events in question, Mr. Chatrie's agreement with Google referred to Location History as "*your*" (meaning, the user's) "information." Under the parties' agreement, too, Mr. Chatrie was free to "review" and "edit" his location data. He was even free to export or delete that data "from Google's servers at will." Beyond all that, Google promised to protect his information against "unauthorized access, alteration, disclosure, or destruction." Put simply, Mr. Chatrie had the rights to enjoy, manage, alter, dispose, and exclude others from what amounted to an electronic diary or map of his travels. And as someone who held that many "sticks in the bundle of rights ... commonly characterized as property"—including the "most treasured" and "essential" right to exclude—he has a strong claim that the Location History data was his personal property.

Next, notice what statutory and case law have to say on the subject. The investigation of Mr. Chatrie unfolded in Virginia. That State's Computer Crimes Act expressly describes "computer data" as a form of "[p]roperty." Va. Code Ann. § 18.2–152.2 (2021).

To be sure, pursuant to its agreement with Mr. Chatrie, Google stored his Location History data on its servers and was free to use it for certain purposes. But an individual need not have "complete ownership or exclusive control" before he can assert a Fourth Amendment challenge against the search of real property. Instead, we have long recognized, a "tenan[t] [or] resident family membe[r]" who does not enjoy "fee simple title" in a house has a sufficient interest in it to give rise to a Fourth Amendment right. And I fail to see why the law should differ markedly when it comes to personal property. If you "[t]oss your keys to a valet at a restaurant" or "[a]sk your neighbor to look after your dog while you travel," you may entrust your personal property to another and license him to do certain things with it, much as Mr. Chatrie did with his Location History data. But that hardly means that property is no longer yours.

Nor does it matter that those who wrote the Fourth Amendment might not have imagined an electronic diary or map of one's travels. As with other laws, the terms found in the Fourth Amendment carry their original public meaning and can bear more applications than its drafters might have expected or intended…

Because Mr. Chatrie's Location History data is his effect, it is subject to the Fourth Amendment's restrictions when the government searches it.

Justice Alito, with whom Justice Thomas joins as to Part I and with whom Justice Barrett joins as to Parts II–B, II–C–1, and II–C–2, dissenting.

I

The Court should not have granted certiorari in this case, and under any faithful application of our precedents, it should now either dismiss this petition or affirm the decision below based on the "good-faith exception" to the exclusionary rule. Instead, the Court issues an advisory opinion concerning a now-obsolete "geofence" procedure. Last Term, the Court worried out loud about rushing in to judge "new technologies with transformative capabilities" that we barely understand.

Advisory-opinion concerns aside, our prudential certiorari considerations further counseled against granting certiorari. Writs of certiorari are discretionary, and we reserve them

for "compelling" cases in which the court below "has decided an important question of federal law." This Court's Rule 10. The question in this case does not qualify.

Chatrie's petition asked whether the geofence procedure that the police used here comports with the Fourth Amendment. The answer to this question has scarcely any ongoing significance. Google, the Government, and the majority all agree that Google has modified its Location History service in a manner that forecloses future use of this geofence procedure. Chatrie does not offer any evidence to the contrary. As a result, Fourth Amendment challenges to this geofence procedure will likely pass into obscurity soon…

II

If the Court were to apply the Fourth Amendment as understood for the first century of this Nation's history, we would find no "search" of Chatrie's papers or effects, much less an "unreasonable" one. Until the last decades of the 19th century, the Search and Seizure Clause protected only the physical security of one's person and property, and document-production orders were not understood to be "searches." Under those principles, Chatrie's arguments are meritless.

To illustrate this point, imagine that Chatrie spent his free time taking road trips across the United States. And suppose that he entered into a contract with a travel agency, under which the agency would provide him valuable information about places to visit and activities to try as he traveled from place to place. If a grand jury had subpoenaed the travel agency for the records of Chatrie's travels, he would have no basis to object on search-and-seizure grounds. At least through the late 19th century, compelled document-production orders were simply not "searches."

Likewise, until *Carpenter*, this Court held that the Fourth Amendment protected a person's security in only his own papers and effects, not those of a third party. Chatrie's claim would therefore fail for a second reason: He possesses no property interest in the information that Google conveyed to the police. To be sure, Chatrie claims a property right in Google's Location History files under a bailor-bailee relationship, and he claims that the execution of the geofence procedure transgressed those rights. This argument radically reconceptualizes the traditional understanding of property rights. And even if Chatrie possessed a property right in the Location History files on Google's servers, the conduct of the police in this case did not infringe that right. The geofence procedure did not give the police access to the Location History files themselves. Rather, Google used the information contained in those files to generate a spreadsheet that summarized objective, historical facts about Chatrie's (and others') location in the hour before and hour after the robbery. The police sought and obtained those historical details, not the files on Google's servers. And whatever property rights Chatrie might have in the Location History files, he does not "own" historical facts about his movements in a given hour. If Chatrie, instead of using Location History, had written and copyrighted a private memoir about his crimes, he would not have a Fourth Amendment claim if the police asked a proofreader whether Chatrie was at the credit union during the robbery. Chatrie therefore cannot show that the police here transgressed any rights in his papers or effects.

In short, under traditional search-and-seizure principles, Chatrie could not challenge the geofence procedure here under the Fourth Amendment.

B

1

Whatever one thinks of *Katz*'s expansion of Fourth Amendment doctrine, this Court at least had the prudence to tread cautiously when implementing that expansion. Indeed, the Court spent much of the 20th century emphasizing the limits of *Katz*'s reach. For instance, the Court held that *Katz* did not require the police to obtain a warrant for visual or physical surveillance outside a house's curtilage. *Oliver* v. *United States* (1984). Nor could a defendant

generally claim an "expectation of privacy" in someone else's home, his own public travels, his face-to-face conversations with another person, or information that he shared with a business. *Minnesota* v. *Carter* (1998); *United States* v. *Knotts* (1983); *United States* v. *White* (1971) (plurality opinion); *Smith* v. *Maryland* (1979). If *Katz* ushered in a revolution in Fourth Amendment doctrine, the Court was quick to cabin its impact. See also *New York* v. *Burger* (1987) (holding that *Katz* does not require a warrant for inspections of "pervasively regulated industries"); *California* v. *Greenwood*, (1988) (holding that *Katz* does not protect privacy interests in household garbage left curbside); *California* v. *Ciraolo*, (1986) (holding that *Katz* does not require a warrant for aerial surveillance).

Similarly, even after *Katz*, the Court recognized that legislatures still bore primary responsibility for regulating the use of new technologies and investigation methods. Thus, when legislatures developed reasonable schemes to administer such activities, the Court was reluctant to constitutionalize additional rules

2

The geofence procedure in this case did not violate Chatrie's Fourth Amendment rights under these 20th-century precedents. These precedents hold that a defendant does not have a reasonable expectation of privacy in records that a company generates by virtue of the defendant's use of its services. This rule has come to be known as the third-party doctrine.

What was true about the bank records in *Miller* is true about Location History here. Chatrie voluntarily conveyed his location information to Google, and Google created a digital paper trail of that information. Like the bank in *Miller*, Google was no neutral custodian in this arrangement. In exchange for allowing Chatrie to use its Location History service, Google could use his location information for its own business purposes, such as sending Chatrie location-targeted advertisements from third parties. So, by giving Google his location information for its own use, Chatrie assumed the risk that Google might disclose location information to others, including the police. Indeed, Google advises its users that the company could use their location information for its own advertising purposes and could share that information with law enforcement. Thus, like the defendant in *Miller*, Chatrie cannot now claim a reasonable expectation of privacy in those data. The police therefore would not need a warrant to perform the geofence procedure under our 20th-century precedents.

C

1

Without any support in 19th- or 20th-century understandings of the Fourth Amendment, Chatrie and the majority rely primarily on this Court's decision in *Carpenter*.

Carpenter maintained that its departure from these [prior] doctrines was "narrow." *Carpenter*'s analysis likewise anchored itself in the "unique nature" of the particular cell-site records that the police had collected in that case.

Three of those aspects—duration, comprehensiveness, and voluntariness—deserve mention here.

2

By its own terms, *Carpenter*'s holding was keyed to the "unique nature" of the cell-site records in that case. *Carpenter* expressly left open the question whether the police would need a warrant for location data spanning less than a week, as is the case with the data here. *Carpenter* likewise declined to address situations where the police request information about all devices in a given area at the time of a crime (*e.g.*, a geofence procedure), as opposed to continuous location information about one specific device. For this reason alone, *Carpenter* does not dictate an outcome here.

Nor does *Carpenter*'s reasoning justify extending its holding to this case. Here, the police requested two pieces of information that could implicate Chatrie's Fourth Amendment interests: (1) whether he was within 150 meters of the credit union during the robbery, and (2) if he was, where he traveled during the 1-hour periods immediately before and afterward. Along three of the dimensions that *Carpenter* found relevant, Chatrie has a far lesser privacy interest in this information than the defendant did in the records at issue in that case. The third-party doctrine therefore controls.

First, unlike the data collection in *Carpenter*, the geofence procedure in this case did not risk uncovering the "whole of [someone's] physical movements." …Second, the limited geofence procedure here was far less likely to open "an intimate window" into Chatrie's " 'familial, political, professional, religious, and sexual associations' " than was the chronicle that the police obtained in *Carpenter*. Third, unlike the generation of cell-site records, the creation of Location History data is voluntary and not integral to a cell phone's functionality. Cell-site records are the by-product of every phone interaction with a cell tower and thus an unavoidable consequence of sending text messages, making phone calls, or connecting to the internet. A person can avoid creating those records only by forgoing all use of a cell phone for these purposes, and doing so would render useless this "indispensable" component of modern life. In contrast, users need not enable Location History for their phones to function as expected. That most Google accountholders carry on without using Location History is strong evidence that the service is not a "pervasive and insistent part of daily life" in the way that creating cell-site records is.

3

The majority reaches the opposite outcome, and in doing so, it announces a new rule of Fourth Amendment law: The police must obtain a warrant every time they access *any* cell-phone location information from a third party, however brief the duration, however innocuous the request, and however voluntarily that information was disclosed by the user. This rule significantly extends *Carpenter* and repudiates the boundary lines that *Carpenter* drew to distinguish its novel holding from longstanding doctrine…. This unshackling of *Carpenter* will unleash the very upheaval in Fourth Amendment law that *Carpenter* disclaimed.

4

In support of its sweeping conclusion, the majority argues that a duration-based or procedure-by-procedure approach to the Fourth Amendment would generate a "host of line-drawing questions." I do not disagree, but those questions are the inevitable byproduct of the lines that *Carpenter* drew when it distinguished away longstanding doctrine. Indeed, the majority's rejection of such line-drawing only betrays its expansion of *Carpenter*'s holding.

In any event, the majority's approach creates its own share of line-drawing problems. What dividing line can explain why a defendant has a reasonable expectation of privacy in his cell-phone location information but not in his bank records? Debit and credit cards might be viewed as comparably "indispensable to participation in modern society," and their use creates a detailed paper trail. As a result, modern bank records contain similarly comprehensive accounts of Americans' private lives, including "the political and religious organizations to which they donate; whether they have visited a psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center; [and] whether they go to gay bars or straight ones." *Id.* (Kennedy, J., dissenting). But as long as *Miller* remains good law, the Fourth Amendment does not require the police to obtain a warrant for these records.[7]

More broadly, where does the boundary between *Carpenter* and the third-party doctrine lie after today? Do the police need a warrant to obtain a person's Amazon purchase history?

[7] One is left wondering on which side of the line location data from a mobile-payment service like Apple Pay falls.

What about a person's Google search history or Venmo transaction log? Those kinds of information fall squarely within the third-party doctrine, and today's holding about "cell phone location information" does not ostensibly disturb that fact. At the same time, those data can paint a similarly detailed picture of a person's private life, and law enforcement had no easy way to obtain this information in "an earlier age." If the Court maintains its unwillingness to engage with such "line-drawing questions," warrant requirement might soon come for all forms of digital surveillance.

Justice Barrett, dissenting.

I have no quarrel with *Carpenter* v. *United States*, 585 U. S. 296 (2018), or with the Court's decision to grant certiorari in this case. But I agree with Justice Alito that under our Fourth Amendment precedent, including *Carpenter*, Chatrie had no reasonable expectation of privacy in data about his public movements that he voluntarily disclosed to Google. I therefore respectfully dissent.

Notes

1. Is the *Chatrie* majority limited to location data? On one hand, the holding is clear: "we hold that police officers invade a cell-phone user's reasonable expectation of privacy when they access his Location History." Yet the majority reference a host of connected services, such as Google Photos and email. Are those also protected? And, if so, is Google Photos protected only on the phone, or is it also protected if images are intentionally uploaded via desktop or laptop?
2. Justice Kagan observes that the *Carpenter* majority "it did not know what further technology was on the horizon." If this is true in any meaningful sense, it is more a condemnation of the *Carpenter* majority than anything else. Everyone knew then that the question of location data held by app providers would soon present itself, just like everyone knows now that the questions in note 1 will present themselves.
3. In addition to his substantive critiques, Justice Alito also criticizes the majority on procedural grounds. In his eyes, the evidence against Chatrie will almost certainly be admitted under the good-faith exception, making the Court's entire analysis little more than an advisory opinion. Worse, the case concerns a discontinued practice; Google claims to no longer be able to fill geofence warrants. Are these critiques fair? Is the advisory opinion critique more applicable here than it was in *Jones*, *Riley*, or *Carpenter*? Scholars have often criticized courts for using the good-faith exception to avoid answering difficult Fourth Amendment questions and to minimize the immediate impact of major changes of law.[87]
4. Gorsuch's concurrence has some seductive appeal. Are these not Chatrie's files? But, as Alito points out, Google had extensive rights to these files, including right to benefit from them in ways that compromised Chatrie's privacy. A fully adoption of Gorsuch's concurrence would require consideration of, first, the contract between consumer and vendor and, second, the general state of American consumer privacy law. This is exactly the kind of analysis that was *not* conducted in *Warshak*, which protected the privacy of email content.

3) Digital Searches

Searches of electronic devices raise a host of issues that are distinct from searches of physical spaces. Most of these turn on the amount of information that can be stored electronically and the difficulty of telling at a glance whether the information is within the scope of a warrant (or, when applicable, warrant exception). Consider a search of a house for an illegal firearm. This search would be limited to a particular location (the house) and particular

[87] See, e.g., Matthew Tokson & Michael Gentithes, *The Reality of the Good Faith Exception*, 113 Geo. L.J. 551 (2025).

spaces in that house (places large enough to hold a firearm). A set of file folders could not be examined under the scope of such a warrant—guns and paper are readily distinguishable.

Consider instead a search of a computer for information about drug dealing. The computer itself may be a physical object, but it has tendrils reaching out into online accounts. These accounts could be for any of a wide range of purposes, and accessing those accounts might involve accessing computers owned by other people and based in other jurisdictions. Further, even the files of a particular computer are mysterious to a searcher. Is evidence of drug dealing found in photo files, spreadsheets, text documents, emails, or all of the above? How does one structure a search strategy that is other than a file-by-file examination of the entire computer?

These questions relate to the particularity of the search. Recall that requirement that warrants be particular comes directly from the text of the Fourth Amendment—this is an important consideration. But we still do not have clear answers on what makes a warrant for an electronic search sufficiently particular.

Think about the investigative steps in the *Riley* case. If the police had filed for a warrant, what would they have said they were looking for? Could a warrant based on probable cause have been issued under these facts?

Riley v. California, 573 U.S. 373 (2014)

ROBERTS delivered the opinion of the Court.

These two cases raise a common question: whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.

In the first case, petitioner David Riley was stopped by a police officer for driving with expired registration tags. In the course of the stop, the officer also learned that Riley's license had been suspended. The officer impounded Riley's car, pursuant to department policy, and another officer conducted an inventory search of the car. Riley was arrested for possession of concealed and loaded firearms when that search turned up two handguns under the car's hood.

An officer searched Riley incident to the arrest and found items associated with the "Bloods" street gang. He also seized a cell phone from Riley's pants pocket. According to Riley's uncontradicted assertion, the phone was a "smart phone," a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity. The officer accessed information on the phone and noticed that some words (presumably in text messages or a contacts list) were preceded by the letters "CK"—a label that, he believed, stood for "Crip Killers," a slang term for members of the Bloods gang.

At the police station about two hours after the arrest, a detective specializing in gangs further examined the contents of the phone. The detective testified that he "went through" Riley's phone "looking for evidence, because . . . gang members will often video themselves with guns or take pictures of themselves with the guns." Although there was "a lot of stuff" on the phone, particular files that "caught [the detective's] eye" included videos of young men sparring while someone yelled encouragement using the moniker "Blood." The police also found photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier.

Riley was ultimately charged, in connection with that earlier shooting, with firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder. Prior to trial, Riley moved to suppress all evidence that the police had obtained from his cell phone. He contended that the searches of his phone violated the Fourth Amendment, because they had been performed without a warrant and were not otherwise justified by exigent circumstances.

In the second case, a police officer performing routine surveillance observed respondent Brima Wurie make an apparent drug sale from a car. Officers subsequently arrested Wurie and

took him to the police station. At the station, the officers seized two cell phones from Wurie's person. The one at issue here was a "flip phone," a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone. Five to ten minutes after arriving at the station, the officers noticed that the phone was repeatedly receiving calls from a source identified as "my house" on the phone's external screen. A few minutes later, they opened the phone and saw a photograph of a woman and a baby set as the phone's wallpaper. They pressed one button on the phone to access its call log, then another button to determine the phone number associated with the "my house" label. They next used an online phone directory to trace that phone number to an apartment building.

When the officers went to the building, they saw Wurie's name on a mailbox and observed through a window a woman who resembled the woman in the photograph on Wurie's phone. They secured the apartment while obtaining a search warrant and, upon later executing the warrant, found and seized 215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash.

Wurie was charged with distributing crack cocaine, possessing crack cocaine with intent to distribute, and being a felon in possession of a firearm and ammunition. He moved to suppress the evidence obtained from the search of the apartment, arguing that it was the fruit of an unconstitutional search of his cell phone.

As the text makes clear, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" Our cases have determined that "[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant."

The two cases before us concern the reasonableness of a warrantless search incident to a lawful arrest. In 1914, this Court first acknowledged in dictum "the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime." *Weeks v. United States*. Since that time, it has been well accepted that such a search constitutes an exception to the warrant requirement.

Three related precedents set forth the rules governing such searches:

The first, *Chimel v. California* (1969), laid the groundwork for most of the existing search incident to arrest doctrine. Police officers in that case arrested Chimel inside his home and proceeded to search his entire three-bedroom house, including the attic and garage. In particular rooms, they also looked through the contents of drawers.

The Court crafted the following rule for assessing the reasonableness of a search incident to arrest:

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction . . . .

The extensive warrantless search of Chimel's home did not fit within this exception, because it was not needed to protect officer safety or to preserve evidence.

Four years later, in *United States v. Robinson* (1973), the Court applied the *Chimel* analysis in the context of a search of the arrestee's person. A police officer had arrested Robinson for driving with a revoked license. The officer conducted a patdown search and felt an object that he could not identify in Robinson's coat pocket. He removed the object, which turned out to be a crumpled cigarette package, and opened it. Inside were 14 capsules of heroin.

The Court thus concluded that the search of Robinson was reasonable even though there was no concern about the loss of evidence, and the arresting officer had no specific concern that Robinson might be armed. It merely noted that, "[h]aving in the course of a lawful search come upon the crumpled package of cigarettes, [the officer] was entitled to inspect it." A few years later, the Court clarified that this exception was limited to "personal property . . . immediately associated with the person of the arrestee." *United States v. Chadwick* (1977) (200–pound, locked footlocker could not be searched incident to arrest).

The search incident to arrest trilogy concludes with *Arizona v. Gant* (2009), which analyzed searches of an arrestee's vehicle. *Gant*, like *Robinson,* recognized that the *Chimel* concerns for officer safety and evidence preservation underlie the search incident to arrest exception. As a result, the Court concluded that *Chimel* could authorize police to search a vehicle "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search." *Gant* added, however, an independent exception for a warrantless search of a vehicle's passenger compartment "when it is 'reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'"

III

These cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy. A smart phone of the sort taken from Riley was unheard of ten years ago; a significant majority of American adults now own such phones. Even less sophisticated phones like Wurie's, which have already faded in popularity since Wurie was arrested in 2007, have been around for less than 15 years. Both phones are based on technology nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided.

Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." Such a balancing of interests supported the search incident to arrest exception in *Robinson,* and a mechanical application of *Robinson* might well support the warrantless searches at issue here.

But while *Robinson* 's categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones. On the government interest side, *Robinson* concluded that the two risks identified in *Chimel*—harm to officers and destruction of evidence—are present in all custodial arrests. There are no comparable risks when the search is of digital data. In addition, *Robinson* regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*.

We therefore decline to extend *Robinson* to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.

A

Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.

The United States and California both suggest that a search of cell phone data might help ensure officer safety in more indirect ways, for example by alerting officers that confederates of the arrestee are headed to the scene . . . but neither the United States nor California offers evidence to suggest that their concerns are based on actual experience.

The United States and California focus primarily on the second *Chimel* rationale: preventing the destruction of evidence.

Both Riley and Wurie concede that officers could have seized and secured their cell phones to prevent destruction of evidence while seeking a warrant. That is a sensible concession. And once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone.

The United States and California argue that information on a cell phone may nevertheless be vulnerable to two types of evidence destruction unique to digital data—remote wiping and data encryption. Remote wiping occurs when a phone, connected to a wireless network, receives a signal that erases stored data. This can happen when a third party sends a remote signal or when a phone is preprogrammed to delete data upon entering or leaving certain geographic areas (so-called "geofencing"). Encryption is a security feature that some modern cell phones use in addition to password protection. When such phones lock, data becomes protected by sophisticated encryption that renders a phone all but "unbreakable" unless police know the password.

We have also been given little reason to believe that either problem is prevalent. The briefing reveals only a couple of anecdotal examples of remote wiping triggered by an arrest. Similarly, the opportunities for officers to search a password-protected phone before data becomes encrypted are quite limited. Law enforcement officers are very unlikely to come upon such a phone in an unlocked state because most phones lock at the touch of a button or, as a default, after some very short period of inactivity.

In any event, as to remote wiping, law enforcement is not without specific means to address the threat. Remote wiping can be fully prevented by disconnecting a phone from the network. There are at least two simple ways to do this: First, law enforcement officers can turn the phone off or remove its battery. Second, if they are concerned about encryption or other potential problems, they can leave a phone powered on and place it in an enclosure that isolates the phone from radio waves. Such devices are commonly called "Faraday bags," after the English scientist Michael Faraday. They are essentially sandwich bags made of aluminum foil: cheap, lightweight, and easy to use.

B

The search incident to arrest exception rests not only on the heightened government interests at stake in a volatile arrest situation, but also on an arrestee's reduced privacy interests upon being taken into police custody. *Robinson* focused primarily on the first of those rationales.

Robinson is the only decision from this Court applying *Chimel* to a search of the contents of an item found on an arrestee's person. Lower courts applying *Robinson* and *Chimel,* however, have approved searches of a variety of personal items carried by an arrestee. See, *e.g., United States v. Carrion* (5th Cir. 1987) (billfold and address book); *United States v. Watson* (11th Cir. 1982) (wallet); *United States v. Lee* (D.C. Cir. 1974) (purse).

The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets

works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in *Chadwick* rather than a container the size of the cigarette package in *Robinson*.

But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones. The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.

The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception.

Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.

Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life.

In 1926, Learned Hand observed that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." *United States v. Kirschenblatt* (2nd Cir.). If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house . . . .

To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing." Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference. Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another.

C

Apart from their arguments for a direct extension of *Robinson*, the United States and California offer various fallback options for permitting warrantless cell phone searches under certain circumstances. Each of the proposals is flawed and contravenes our general preference to provide clear guidance to law enforcement through categorical rules.

The United States first proposes that the *Gant* standard be imported from the vehicle context, allowing a warrantless search of an arrestee's cell phone whenever it is reasonable to believe that the phone contains evidence of the crime of arrest. [But] a *Gant* standard would prove no practical limit at all when it comes to cell phone searches. In the vehicle context, *Gant* generally protects against searches for evidence of past crimes. In the cell phone context, however, it is reasonable to expect that incriminating information will be found on a phone regardless of when the crime occurred. The sources of potential pertinent information are virtually unlimited, so applying the *Gant* standard to cell phones would in effect give "police officers unbridled discretion to rummage at will among a person's private effects."

The United States also proposes a rule that would restrict the scope of a cell phone search to those areas of the phone where an officer reasonably believes that information relevant to the crime, the arrestee's identity, or officer safety will be discovered. This approach would again impose few meaningful constraints on officers.

We also reject the United States' final suggestion that officers should always be able to search a phone's call log, as they did in Wurie's case. The Government relies on *Smith v. Maryland* (1979), which held that no warrant was required to use a pen register at telephone company premises to identify numbers dialed by a particular caller. The Court in that case, however, concluded that the use of a pen register was not a "search" at all under the Fourth Amendment There is no dispute here that the officers engaged in a search of Wurie's cell phone. Moreover, call logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label "my house" in Wurie's case.

Finally, at oral argument California suggested a different limiting principle, under which officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart. But the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years.

IV

We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.

Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest.

Moreover, even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone. "One well-recognized exception applies when "'the exigencies of the situation" make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.'"

In light of the availability of the exigent circumstances exception, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone.

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.

Justice ALITO, concurring in part and concurring in the judgment.

I agree with the Court that law enforcement officers, in conducting a lawful search incident to arrest, must generally obtain a warrant before searching information stored or accessible on a cell phone. I write separately to address two points.

First, I am not convinced at this time that the ancient rule on searches incident to arrest is based exclusively (or even primarily) on the need to protect the safety of arresting officers and the need to prevent the destruction of evidence. On the contrary, when pre-*Weeks v. United States* (1914) authorities discussed the basis for the rule, what was mentioned was the need to obtain probative evidence. The idea that officer safety and the preservation of evidence are the sole reasons for allowing a warrantless search incident to arrest appears to derive from the Court's reasoning in *Chimel v. California* (1969), a case that involved the lawfulness of a search of the scene of an arrest, not the person of an arrestee.

Despite my view on the point discussed above, I agree that we should not mechanically apply the rule used in the predigital era to the search of a cell phone. Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form. This calls for a new balancing of law enforcement and privacy interests.

While the Court's approach leads to anomalies, I do not see a workable alternative. Law enforcement officers need clear rules regarding searches incident to arrest, and it would take many cases and many years for the courts to develop more nuanced rules. And during that time, the nature of the electronic devices that ordinary Americans carry on their persons would continue to change.

This brings me to my second point. While I agree with the holding of the Court, I would reconsider the question presented here if either Congress or state legislatures, after assessing

the legitimate needs of law enforcement and the privacy interests of cell phone owners, enact legislation that draws reasonable distinctions based on categories of information or perhaps other variables.

Notes

1. *Riley* is the first of Roberts' two "cellphones are special" cases. The other is *Carpenter*. In both cases there is a focus on the unique role that cellphones play in modern life and the unique challenges posed by their vast storage capacities. In the years since these opinions, has Roberts become more or less right about the role of cellphones? In what direction is this headed?
2. How difficult is it to "get a warrant" in a case like these? Is the main effect of *Riley* that it will be slightly less convenient to conduct casual searches of seized electronics? Or are there cases where the police will not be able to conduct searches even if they are willing to bear the cost of filling out the paperwork?
3. Alito has a plaintive call at the end of his concurrence asking Congress to please legislate on this issue. It has not. In the wake of *Katz* and *Smith*, Congress passed the various versions of the Electronic Communications Privacy Act (See Chapter 3.D). Why do you think there has not been similar work after *Jones*, *Riley*, and *Carpenter*?

C. Constitutional limitations on non-law enforcement searches

The question of "what is a search?" operates the same under the Fourth Amendment for both the law enforcement and non-law enforcement contexts. The consequences of concluding that an action is a search are different, however.[88] In the traditional law enforcement context, courts default to requiring a warrant based on probable cause (or one of the specific exceptions to the warrant requirement). When the goal of a search is not criminal law enforcement, when it is instead a "special needs" search, courts appear to assume that it is less problematic and less intrusive to conduct surveillance.[89] Courts evaluating a non-law enforcement "search" therefore conduct a reasonableness balancing analysis that weighs the intrusiveness of the search against the expected government benefits of that search rather than requiring probable cause and a warrant.

The basic logic is that there are non-law enforcement situations in which the Fourth Amendment warrant and probable cause requirements are "impracticable." In these instances, the warrant requirement may be relaxed, such that a lesser amount of individualized suspicion is required and judicial pre-approval is not necessary. A search based on no individualized suspicion (a dragnet) may also be reasonable "[i]n limited circumstances, where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion . . . ."[90]

Many special needs searches are of people who, by virtue of their status or activities, have reduced expectations of privacy. The canonical examples are public school students and government employees. "[S]tudents within the school environment have a lesser expectation of

[88] Much of the following section is adapted from Matthew B. Kugler & Mariana Oliver, *Constitutional Pandemic Surveillance,* 111 J. CRIM. L. & CRIMINOLOGY 909 (2021).

[89] *See, e.g.*, *Camara v. Mun. Ct. of the City & Cnty. of S.F.*, 387 U.S. 523, 530 (1967) ("We may agree that a routine inspection of the physical condition of private property is a less hostile intrusion than the typical policeman's search for the fruits and instrumentalities of crime.").

[90] *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 624 (1989).

privacy than members of the population generally" and can be subjected to a variety of intrusions in the form of a search or seizure.[91] Student athletes have further reduced expectations, as they have voluntarily chosen to seek the benefits of an extracurricular program.[92] The Supreme Court has used similar logic in the government employment context. It has explained that the "operational realities of the workplace" make it unreasonable for public employees to expect the same level of privacy protections as everyday citizens.[93] Those government employees who have or are seeking positions of particular trust and confidence have further reduced expectations based on their voluntary pursuit of those positions.[94]

Suspicionless dragnet stops of drivers at checkpoints are constitutional under the right circumstances. This is in part because of the special status of automobiles. Though automobile ownership is widespread and travel by car is almost universal,[95] automotive travel has always been treated as a special case. Automobiles are held to be subject to reduced expectations of privacy not just from their various characteristics (ready mobility, large windows, travel in public spaces), but also due to the intrusive regulation imposed on them itself; people should know better (in the view of courts) than to expect privacy in such a regulated device.[96]

Further, such checkpoints have to comply with certain rules. First, they must be for purposes other than the detection of ordinary criminal wrongdoing.[97] When the purpose is general crime control—such as mass license and registration checks—the Court "decline[s] to suspend the usual requirement of individualized suspicion."[98] Second, these checkpoint stops must be brief. This is consistent with the comment in *Skinner v. Railway. Labor Executives' Association* (1989) that the privacy intrusions of dragnet searches should be "minimal."[99] The Supreme Court has therefore approved sobriety checkpoints aimed at removing drunk drivers from the road,[100] brief information-seeking stops to search for witnesses to a hit-and-run,[101] and searches of vehicles near the national border to intercept undocumented migrants.[102]

Vernonia School Dist. 47J v. Acton, 515 U.S. 646 (1995)

Justice SCALIA delivered the opinion of the Court.

Petitioner Vernonia School District 47J (District) operates one high school and three grade schools in the logging community of Vernonia, Oregon. As elsewhere in small-town

---

[91] *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 656–57 (1995) (quoting *New Jersey v. T.L.O.*, 469 U.S. 325, 348 (1985) (Powell, J., concurring)).

[92] *Id.* at 657 (likening student athletes to a "closely regulated industry").

[93] *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987).

[94] *See Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 670 (1989) ("It is readily apparent that the Government has a compelling interest in ensuring that front-line interdiction personnel are physically fit, and have unimpeachable integrity and judgment.").

[95] Sarah Seo has described how the combination of automobiles and Prohibition led to the first widespread encounters between law enforcement and everyday citizens. "It was significant that Prohibitions' offenders were not limited to the unsavory sort." SARAH SEO, POLICING THE OPEN ROAD, 118–120 (2019).

[96] *Ill. v. Lidster*, 540 U.S. 419, 424–25 (2004); *Cal. v. Carney*, 471 U.S. 386, 392 (1985) ("These reduced expectations of privacy derive not from the fact that the area to be searched is in plain view, but from the pervasive regulation of vehicles capable of traveling on the public highways.").

[97] *City of Indianapolis v. Edmond*, 531 U.S. 32, 37–38 (2000) ("[W]e have upheld certain regimes of suspicionless searches where the program was designed to serve 'special needs, beyond the normal need for law enforcement.' In none of these cases, however, did we indicate approval of a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing.").

[98] *Id.* at 44.

[99] 489 U.S. at 624.

[100] *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 447 (1990).

[101] *Lidster*, 540 U.S. at 421.

[102] *U.S. v. Martinez-Fuerte*, 428 U.S. 543, 545 (1976).

America, school sports play a prominent role in the town's life, and student athletes are admired in their schools and in the community.

Drugs had not been a major problem in Vernonia schools. In the mid-to-late 1980's, however, teachers and administrators observed a sharp increase in drug use. Students began to speak out about their attraction to the drug culture, and to boast that there was nothing the school could do about it. Along with more drugs came more disciplinary problems. Between 1988 and 1989 the number of disciplinary referrals in Vernonia schools rose to more than twice the number reported in the early 1980s, and several students were suspended. Students became increasingly rude during class; outbursts of profane language became common.

Not only were student athletes included among the drug users but, as the District Court found, athletes were the leaders of the drug culture. This caused the District's administrators particular concern, since drug use increases the risk of sports-related injury. Expert testimony at the trial confirmed the deleterious effects of drugs on motivation, memory, judgment, reaction, coordination, and performance. The high school football and wrestling coach witnessed a severe sternum injury suffered by a wrestler, and various omissions of safety procedures and misexecutions by football players, all attributable in his belief to the effects of drug use.

Initially, the District responded to the drug problem by offering special classes, speakers, and presentations designed to deter drug use. It even brought in a specially trained dog to detect drugs, but the drug problem persisted.

At that point, District officials began considering a drug-testing program. They held a parent “input night” to discuss the proposed Student Athlete Drug Policy (Policy), and the parents in attendance gave their unanimous approval. The school board approved the Policy for implementation in the fall of 1989. Its expressed purpose is to prevent student athletes from using drugs, to protect their health and safety, and to provide drug users with assistance programs.

The Policy applies to all students participating in interscholastic athletics. Students wishing to play sports must sign a form consenting to the testing and must obtain the written consent of their parents. Athletes are tested at the beginning of the season for their sport. In addition, once each week of the season the names of the athletes are placed in a “pool” from which a student, with the supervision of two adults, blindly draws the names of 10% of the athletes for random testing. Those selected are notified and tested that same day, if possible.

The student to be tested completes a specimen control form which bears an assigned number. Prescription medications that the student is taking must be identified by providing a copy of the prescription or a doctor's authorization. The student then enters an empty locker room accompanied by an adult monitor of the same sex. Each boy selected produces a sample at a urinal, remaining fully clothed with his back to the monitor, who stands approximately 12 to 15 feet behind the student. Monitors may (though do not always) watch the student while he produces the sample, and they listen for normal sounds of urination. Girls produce samples in an enclosed bathroom stall, so that they can be heard but not observed. After the sample is produced, it is given to the monitor, who checks it for temperature and tampering and then transfers it to a vial.

The samples are sent to an independent laboratory, which routinely tests them for amphetamines, cocaine, and marijuana. Other drugs, such as LSD, may be screened at the request of the District, but the identity of a particular student does not determine which drugs will be tested. The laboratory's procedures are 99.94% accurate. The District follows strict procedures regarding the chain of custody and access to test results. The laboratory does not know the identity of the students whose samples it tests. It is authorized to mail written test reports only to the superintendent and to provide test results to District personnel by telephone only after the requesting official recites a code confirming his authority. Only the

superintendent, principals, vice-principals, and athletic directors have access to test results, and the results are not kept for more than one year.

If a sample tests positive, a second test is administered as soon as possible to confirm the result. If the second test is negative, no further action is taken. If the second test is positive, the athlete's parents are notified, and the school principal convenes a meeting with the student and his parents, at which the student is given the option of (1) participating for six weeks in an assistance program that includes weekly urinalysis, or (2) suffering suspension from athletics for the remainder of the current season and the next athletic season. The student is then retested prior to the start of the next athletic season for which he or she is eligible. The Policy states that a second offense results in automatic imposition of option (2); a third offense in suspension for the remainder of the current season and the next two athletic seasons.

In the fall of 1991, respondent James Acton, then a seventh grader, signed up to play football at one of the District's grade schools. He was denied participation, however, because he and his parents refused to sign the testing consent forms.

As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is "reasonableness." At least in a case such as this, where there was no clear practice, either approving or disapproving the type of search at issue, at the time the constitutional provision was enacted, whether a particular search meets the reasonableness standard "'is judged by balancing the intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'" Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, this Court has said that reasonableness generally requires the obtaining of a judicial warrant. Warrants cannot be issued, of course, without the showing of probable cause required by the Warrant Clause. But a warrant is not required to establish the reasonableness of *all* government searches; and when a warrant is not required (and the Warrant Clause therefore not applicable), probable cause is not invariably required either. A search unsupported by probable cause can be constitutional, we have said, "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."

We have found such "special needs" to exist in the public school context. There, the warrant requirement "would unduly interfere with the maintenance of the swift and informal disciplinary procedures [that are] needed," and "strict adherence to the requirement that searches be based upon probable cause" would undercut "the substantial need of teachers and administrators for freedom to maintain order in the schools." *T.L.O.* The school search we approved in *T.L.O.*, while not based on probable cause, *was* based on individualized *suspicion* of wrongdoing. As we explicitly acknowledged, however, "'the Fourth Amendment imposes no irreducible requirement of such suspicion.'" We have upheld suspicionless searches and seizures to conduct drug testing of railroad personnel involved in train accidents, to conduct random drug testing of federal customs officers who carry arms or are involved in drug interdiction. and to maintain automobile checkpoints looking for illegal immigrants and contraband, and drunk drivers.

The first factor to be considered is the nature of the privacy interest upon which the search here at issue intrudes. Central, in our view, to the present case is the fact that the subjects of the Policy are (1) children, who (2) have been committed to the temporary custody of the State as schoolmaster.

Traditionally at common law, and still today, unemancipated minors lack some of the most fundamental rights of self-determination—including even the right of liberty in its narrow sense, *i.e.,* the right to come and go at will. They are subject, even as to their physical freedom, to the control of their parents or guardians. When parents place minor children in private schools for their education, the teachers and administrators of those schools stand *in loco parentis* over the children entrusted to them.

In *T.L.O.* we rejected the notion that public schools, like private schools, exercise only parental power over their students, which of course is not subject to constitutional constraints. But while denying that the State's power over schoolchildren is formally no more than the delegated power of their parents, *T.L.O.* did not deny, but indeed emphasized, that the nature of that power is custodial and tutelary, permitting a degree of supervision and control that could not be exercised over free adults. "[A] proper educational environment requires close supervision of schoolchildren, as well as the enforcement of rules against conduct that would be perfectly permissible if undertaken by an adult." Thus, while children assuredly do not "shed their constitutional rights . . . at the schoolhouse gate," *Tinker v. Des Moines Indep. Cmty. Sch. Dist.* (1969), the nature of those rights is what is appropriate for children in school.

Fourth Amendment rights, no less than First and Fourteenth Amendment rights, are different in public schools than elsewhere; the "reasonableness" inquiry cannot disregard the schools' custodial and tutelary responsibility for children. For their own good and that of their classmates, public school children are routinely required to submit to various physical examinations, and to be vaccinated against various diseases. According to the American Academy of Pediatrics, most public schools "provide vision and hearing screening and dental and dermatological checks . . . . Others also mandate scoliosis screening at appropriate grade levels." In the 1991–1992 school year, all 50 States required public school students to be vaccinated against diphtheria, measles, rubella, and polio. Particularly with regard to medical examinations and procedures, therefore, "students within the school environment have a lesser expectation of privacy than members of the population generally."

Legitimate privacy expectations are even less with regard to student athletes. School sports are not for the bashful. They require "suiting up" before each practice or event, and showering and changing afterwards. Public school locker rooms, the usual sites for these activities, are not notable for the privacy they afford. The locker rooms in Vernonia are typical: No individual dressing rooms are provided; shower heads are lined up along a wall, unseparated by any sort of partition or curtain; not even all the toilet stalls have doors. As the United States Court of Appeals for the Seventh Circuit has noted, there is "an element of 'communal undress' inherent in athletic participation."

There is an additional respect in which school athletes have a reduced expectation of privacy. By choosing to "go out for the team," they voluntarily subject themselves to a degree of regulation even higher than that imposed on students generally. In Vernonia's public schools, they must submit to a preseason physical exam James testified that his included the giving of a urine sample, they must acquire adequate insurance coverage or sign an insurance waiver, maintain a minimum grade point average, and comply with any "rules of conduct, dress, training hours and related matters as may be established for each sport by the head coach and athletic director with the principal's approval." Somewhat like adults who choose to participate in a "closely regulated industry," students who voluntarily participate in school athletics have reason to expect intrusions upon normal rights and privileges, including privacy.

Having considered the scope of the legitimate expectation of privacy at issue here, we turn next to the character of the intrusion that is complained of. We recognized in *Skinner v. Railway. Labor Executives' Association* (1989) that collecting the samples for urinalysis intrudes upon "an excretory function traditionally shielded by great privacy." We noted, however, that the degree of intrusion depends upon the manner in which production of the urine sample is monitored. Under the District's Policy, male students produce samples at a urinal along a wall. They remain fully clothed and are only observed from behind, if at all. Female students produce samples in an enclosed stall, with a female monitor standing outside listening only for sounds of tampering. Under such conditions, the privacy interests compromised by the process of obtaining the urine sample are in our view negligible.

The other privacy-invasive aspect of urinalysis is, of course, the information it discloses concerning the state of the subject's body, and the materials he has ingested. In this regard it

is significant that the tests at issue here look only for drugs, and not for whether the student is, for example, epileptic, pregnant, or diabetic.

Respondents argue, however, that the District's Policy is in fact more intrusive than this suggests, because it requires the students, if they are to avoid sanctions for a falsely positive test, to identify *in advance* prescription medications they are taking. We agree that this raises some cause for concern. On the other hand, we have never indicated that requiring advance disclosure of medications is *per se* unreasonable.

Finally, we turn to consider the nature and immediacy of the governmental concern at issue here, and the efficacy of this means for meeting it.

As for the immediacy of the District's concerns: We are not inclined to question—indeed, we could not possibly find clearly erroneous—the District Court's conclusion that "a large segment of the student body, particularly those involved in interscholastic athletics, was in a state of rebellion," that "[d]isciplinary actions had reached 'epidemic proportions,'" and that "the rebellion was being fueled by alcohol and drug abuse as well as by the student's misperceptions about the drug culture."

As to the efficacy of this means for addressing the problem: It seems to us self-evident that a drug problem largely fueled by the "role model" effect of athletes' drug use, and of particular danger to athletes, is effectively addressed by making sure that athletes do not use drugs. Respondents argue that a "less intrusive means to the same end" was available, namely, "drug testing on suspicion of drug use." We have repeatedly refused to declare that only the "least intrusive" search practicable can be reasonable under the Fourth Amendment.

Taking into account all the factors we have considered above—the decreased expectation of privacy, the relative unobtrusiveness of the search, and the severity of the need met by the search—we conclude Vernonia's Policy is reasonable and hence constitutional.

We caution against the assumption that suspicionless drug testing will readily pass constitutional muster in other contexts. The most significant element in this case is the first we discussed: that the Policy was undertaken in furtherance of the government's responsibilities, under a public school system, as guardian and tutor of children entrusted to its care.

Justice GINSBURG, concurring.

The Court constantly observes that the School District's drug-testing policy applies only to students who voluntarily participate in interscholastic athletics. Correspondingly, the most severe sanction allowed under the District's policy is suspension from extracurricular athletic programs. I comprehend the Court's opinion as reserving the question whether the District, on no more than the showing made here, constitutionally could impose routine drug testing not only on those seeking to engage with others in team sports, but on all students required to attend school.

Justice O'CONNOR, with whom Justice STEVENS and Justice SOUTER join, dissenting.

The population of our Nation's public schools, grades 7 through 12, numbers around 18 million. By the reasoning of today's decision, the millions of these students who participate in interscholastic sports, an overwhelming majority of whom have given school officials no reason whatsoever to suspect they use drugs at school, are open to an intrusive bodily search.

In justifying this result, the Court dispenses with a requirement of individualized suspicion on considered policy grounds. First, it explains that precisely because *every* student athlete is being tested, there is no concern that school officials might act arbitrarily in choosing whom to test. Second, a broad-based search regime, the Court reasons, dilutes the accusatory nature of the search. In making these policy arguments, of course, the Court sidesteps powerful, countervailing privacy concerns. Blanket searches, because they can involve "thousands or

millions" of searches, "pos[e] a greater threat to liberty" than do suspicion-based ones, which "affec[t] one person at a time." Searches based on individualized suspicion also afford potential targets considerable control over whether they will, in fact, be searched because a person can avoid such a search by not acting in an objectively suspicious way. And given that the surest way to avoid acting suspiciously is to avoid the underlying wrongdoing, the costs of such a regime, one would think, are minimal.

The view that mass, suspicionless searches, however evenhanded, are generally unreasonable remains inviolate in the criminal law enforcement context, at least where the search is more than minimally intrusive. We have not hesitated to treat monitored bowel movements as highly intrusive (even in the special border search context), and it is not easy to draw a distinction. And certainly monitored urination combined with urine testing is more intrusive than some personal searches we have said trigger Fourth Amendment protections in the past.

Outside the criminal context, however, in response to the exigencies of modern life, our cases have upheld several evenhanded blanket searches, including some that are more than minimally intrusive, after balancing the invasion of privacy against the government's strong need. Most of these cases, of course, are distinguishable insofar as they involved searches either not of a personally intrusive nature, such as searches of closely regulated businesses, or arising in unique contexts such as prisons.

The instant case stands in marked contrast. One searches today's majority opinion in vain for recognition that history and precedent establish that individualized suspicion is "usually required" under the Fourth Amendment (regardless of whether a warrant and probable cause are also required) and that, in the area of intrusive personal searches, the only recognized exception is for situations in which a suspicion-based scheme would be likely ineffectual. Far from acknowledging anything special about individualized suspicion, the Court treats a suspicion-based regime as if it were just any run-of-the-mill, less intrusive alternative—that is, an alternative that officials may bypass if the lesser intrusion, in their reasonable estimation, is outweighed by policy concerns unrelated to practicability.

The record here indicates that the Vernonia schools are no exception. The great irony of this case is that most (though not all) of the evidence the District introduced to justify its suspicionless drug testing program consisted of first- or second-hand stories of particular, identifiable students acting in ways that plainly gave rise to reasonable suspicion of in-school drug use—and thus that would have justified a drug-related search under our *T.L.O.* decision. Small groups of students, for example, were observed by a teacher "passing joints back and forth" across the street at a restaurant before school and during school hours. Another group was caught skipping school and using drugs at one of the students' houses.

In light of all this evidence of drug use by particular students, there is a substantial basis for concluding that a vigorous regime of suspicion-based testing (for which the District appears already to have rules in place) would have gone a long way toward solving Vernonia's school drug problem while preserving the Fourth Amendment rights of James Acton and others like him.

I find unpersuasive the Court's reliance on the widespread practice of physical examinations and vaccinations, which are both blanket searches of a sort. It might also be noted that physical exams (and of course vaccinations) are not searches for conditions that reflect wrongdoing on the part of the student, and so are *wholly* nonaccusatory and have no consequences that can be regarded as punitive. These facts may explain the absence of Fourth Amendment challenges to such searches.

I do not believe that suspicionless drug testing is justified on these facts. But even if I agreed that some such testing were reasonable here, I see two other Fourth Amendment flaws in the District's program. First, and most serious, there is virtually no evidence in the record of

a drug problem at the Washington Grade School, which includes the seventh and eighth grades, and which Acton attended when this litigation began.

Second, even as to the high school, I find unreasonable the school's choice of student athletes as the class to subject to suspicionless testing—a choice that appears to have been driven more by a belief in what would pass constitutional muster, see Transcript (indicating that the original program was targeted at students involved in any extracurricular activity), than by a belief in what was required to meet the District's principal disciplinary concern.

Notes

1. How should we think about degree of intrusion in a case like this? The Court emphasized that the actual collection of the urine sample was relatively inoffensive, with athletes forced into no greater exposure than was common in communal restrooms. It specifically called the privacy interests "negligible." Is that right?
2. In concurrence, Justice Ginsburg stresses that this case does not concern a general program of student drug testing. *In Board of Education v. Earls*, 536 U.S. 822 (2002), the Court upheld drug testing of all students engaged in extracurriculars. Which of the Court's rationales in *Acton* are substantially weaker when applied to this broad program? Are the remaining factors—specifically the weak privacy protections of students, the voluntary nature of extracurriculars, and the minimal intrusion of the program—sufficient to justify it?
3. School resource officers (SROs) are law enforcement officials trained in "school-based law enforcement" and assigned to work with one or more schools. These officers almost uniformly carry firearms and often make arrests without the input of school officials. Courts have differed in their approaches for determining whether searches conducted by SRO are special needs searches. For example, if a search is a collaboration between a school official and an SRO some courts have focused on who initiated the search, finding that a search initiated by a school official falls into the special need exception even if an SRO is involved, whereas others have focused on the purpose of the search, with the latter approach generally being preferred by scholars.

Whereas *Acton* focuses on the nature of the relationship between the government and the students, other cases have turned on different considerations. The emphasis on purposes beyond general crime control is central in one of the few special needs cases that is about public health: *Ferguson v. City of Charleston*.

Ferguson v. City of Charleston, 532 U.S. 67 (2001)

Justice STEVENS delivered the opinion of the Court.

In this case, we must decide whether a state hospital's performance of a diagnostic test to obtain evidence of a patient's criminal conduct for law enforcement purposes is an unreasonable search if the patient has not consented to the procedure. More narrowly, the question is whether the interest in using the threat of criminal sanctions to deter pregnant women from using cocaine can justify a departure from the general rule that an official nonconsensual search is unconstitutional if not authorized by a valid warrant.

In the fall of 1988, staff members at the public hospital operated in the city of Charleston by the Medical University of South Carolina (MUSC) became concerned about an apparent increase in the use of cocaine by patients who were receiving prenatal treatment. In response to this perceived increase, as of April 1989, MUSC began to order drug screens to be performed on urine samples from maternity patients who were suspected of using cocaine. If a patient tested positive, she was then referred by MUSC staff to the county substance abuse commission for counseling and treatment. However, despite the referrals, the incidence of cocaine use among the patients at MUSC did not appear to change.

Some four months later, Nurse Shirley Brown, the case manager for the MUSC obstetrics department, heard a news broadcast reporting that the police in Greenville, South Carolina, were arresting pregnant users of cocaine on the theory that such use harmed the fetus and was therefore child abuse. Nurse Brown discussed the story with MUSC's general counsel, Joseph C. Good, Jr., who then contacted Charleston Solicitor Charles Condon in order to offer MUSC's cooperation in prosecuting mothers whose children tested positive for drugs at birth.

After receiving Good's letter, Solicitor Condon took the first steps in developing the policy at issue in this case. He organized the initial meetings, decided who would participate, and issued the invitations, in which he described his plan to prosecute women who tested positive for cocaine while pregnant. The task force that Condon formed included representatives of MUSC, the police, the County Substance Abuse Commission and the Department of Social Services. Their deliberations led to MUSC's adoption of a 12–page document entitled "POLICY M–7," dealing with the subject of "Management of Drug Abuse During Pregnancy."

The first section, entitled the "Identification of Drug Abusers," provided that a patient should be tested for cocaine through a urine drug screen if she met one or more of nine criteria [AU note: generally, lack of or inconsistent prenatal care, prior drug use, or congenital abnormalities]. It also stated that a chain of custody should be followed when obtaining and testing urine samples, presumably to make sure that the results could be used in subsequent criminal proceedings. The policy also provided for education and referral to a substance abuse clinic for patients who tested positive. Most important, it added the threat of law enforcement intervention that "provided the necessary 'leverage' to make the [p]olicy effective." That threat was, as respondents candidly acknowledge, essential to the program's success in getting women into treatment and keeping them there.

The threat of law enforcement involvement was set forth in two protocols, the first dealing with the identification of drug use during pregnancy, and the second with identification of drug use after labor. Under the latter protocol, the police were to be notified without delay and the patient promptly arrested. Under the former, after the initial positive drug test, the police were to be notified (and the patient arrested) only if the patient tested positive for cocaine a second time or if she missed an appointment with a substance abuse counselor. In 1990, however, the policy was modified at the behest of the solicitor's office to give the patient who tested positive during labor, like the patient who tested positive during a prenatal care visit, an opportunity to avoid arrest by consenting to substance abuse treatment.

The last six pages of the policy contained forms for the patients to sign, as well as procedures for the police to follow when a patient was arrested. The policy also prescribed in detail the precise offenses with which a woman could be charged, depending on the stage of her pregnancy. [T]he policy made no mention of any change in the prenatal care of such patients, nor did it prescribe any special treatment for the newborns.

Petitioners are 10 women who received obstetrical care at MUSC and who were arrested after testing positive for cocaine. Four of them were arrested during the initial implementation of the policy; they were not offered the opportunity to receive drug treatment as an alternative to arrest. The others were arrested after the policy was modified in 1990; they either failed to comply with the terms of the drug treatment program or tested positive for a second time. Respondents include the city of Charleston, law enforcement officials who helped develop and enforce the policy, and representatives of MUSC.

[T]he majority of the appellate panel held that the searches were reasonable as a matter of law under our line of cases recognizing that "special needs" may, in certain exceptional circumstances, justify a search policy designed to serve non-law enforcement ends. On the understanding "that MUSC personnel conducted the urine drug screens for medical purposes wholly independent of an intent to aid law enforcement efforts," the majority applied the balancing test used in *Treasury Emps. v. Von Raab* (1989) and *Vernonia Sch. Dist. 47J v. Acton*

(1995), and concluded that the interest in curtailing the pregnancy complications and medical costs associated with maternal cocaine use outweighed what the majority termed a minimal intrusion on the privacy of the patients.

We granted certiorari to review the appellate court's holding on the "special needs" issue. Because we do not reach the question of the sufficiency of the evidence with respect to consent, we necessarily assume for purposes of our decision—as did the Court of Appeals—that the searches were conducted without the informed consent of the patients. We conclude that the judgment should be reversed and the case remanded for a decision on the consent issue.

Because MUSC is a state hospital, the members of its staff are government actors, subject to the strictures of the Fourth Amendment. Moreover, the urine tests conducted by those staff members were indisputably searches within the meaning of the Fourth Amendment. Neither the District Court nor the Court of Appeals concluded that any of the nine criteria used to identify the women to be searched provided either probable cause to believe that they were using cocaine, or even the basis for a reasonable suspicion of such use.

Because the hospital seeks to justify its authority to conduct drug tests and to turn the results over to law enforcement agents without the knowledge or consent of the patients, this case differs from the four previous cases in which we have considered whether comparable drug tests "fit within the closely guarded category of constitutionally permissible suspicionless searches." In three of those cases, we sustained drug tests for railway employees involved in train accidents, *Skinner v. Ry. Lab. Execs.' Ass'n* (1989), for United States Customs Service employees seeking promotion to certain sensitive positions, *Treasury Emps. v. Von Raab* (1989), and for high school students participating in interscholastic sports, *Vernonia Sch. Dist. 47J v. Acton* (1995). In the fourth case, we struck down such testing for candidates for designated state offices as unreasonable. *Chandler v. Miller* (1997).

In each of those cases, we employed a balancing test that weighed the intrusion on the individual's interest in privacy against the "special needs" that supported the program. As an initial matter, we note that the invasion of privacy in this case is far more substantial than in those cases. In the previous four cases, there was no misunderstanding about the purpose of the test or the potential use of the test results, and there were protections against the dissemination of the results to third parties. The use of an adverse test result to disqualify one from eligibility for a particular benefit, such as a promotion or an opportunity to participate in an extracurricular activity, involves a less serious intrusion on privacy than the unauthorized dissemination of such results to third parties. The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.

The critical difference between those four drug-testing cases and this one, however, lies in the nature of the "special need" asserted as justification for the warrantless searches. In each of those earlier cases, the "special need" that was advanced as a justification for the absence of a warrant or individualized suspicion was one divorced from the State's general interest in law enforcement. In this case, however, the central and indispensable feature of the policy from its inception was the use of law enforcement to coerce the patients into substance abuse treatment. This fact distinguishes this case from circumstances in which physicians or psychologists, in the course of ordinary medical procedures aimed at helping the patient herself, come across information that under rules of law or ethics is subject to reporting requirements, which no one has challenged here.

Respondents argue in essence that their ultimate purpose—namely, protecting the health of both mother and child—is a beneficent one. In *Chandler*, however, we did not simply accept the State's invocation of a "special need." Instead, we carried out a "close review" of the scheme at issue before concluding that the need in question was not "special," as that term has been defined in our cases. In this case, a review of the [] policy plainly reveals that the purpose

actually served by the MUSC searches "is ultimately indistinguishable from the general interest in crime control."

Moreover, throughout the development and application of the policy, the Charleston prosecutors and police were extensively involved in the day-to-day administration of the policy. Police took pains to coordinate the timing and circumstances of the arrests with MUSC staff, and, in particular, Nurse Brown.

While the ultimate goal of the program may well have been to get the women in question into substance abuse treatment and off of drugs, the immediate objective of the searches was to generate evidence *for law enforcement purposes* in order to reach that goal. The threat of law enforcement may ultimately have been intended as a means to an end, but the direct and primary purpose of MUSC's policy was to ensure the use of those means. In our opinion, this distinction is critical. Because law enforcement involvement always serves some broader social purpose or objective, under respondents' view, virtually any nonconsensual suspicionless search could be immunized under the special needs doctrine by defining the search solely in terms of its ultimate, rather than immediate, purpose. Such an approach is inconsistent with the Fourth Amendment. Given the primary purpose of the Charleston program, which was to use the threat of arrest and prosecution in order to force women into treatment, and given the extensive involvement of law enforcement officials at every stage of the policy, this case simply does not fit within the closely guarded category of "special needs."

As respondents have repeatedly insisted, their motive was benign rather than punitive. Such a motive, however, cannot justify a departure from Fourth Amendment protections, given the pervasive involvement of law enforcement with the development and application of the MUSC policy. The stark and unique fact that characterizes this case is that Policy M–7 was designed to obtain evidence of criminal conduct by the tested patients that would be turned over to the police and that could be admissible in subsequent criminal prosecutions. While respondents are correct that drug abuse both was and is a serious problem, "the gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose." *City of Indianapolis v. Edmond* (2000). The Fourth Amendment's general prohibition against nonconsensual, warrantless, and suspicionless searches necessarily applies to such a policy.

Accordingly, the judgment of the Court of Appeals is reversed, and the case is remanded for further proceedings consistent with this opinion.

Justice SCALIA, dissenting.

There is always an unappealing aspect to the use of doctors and nurses, ministers of mercy, to obtain incriminating evidence against the supposed objects of their ministration—although here, it is correctly pointed out, the doctors and nurses were ministering not just to the mothers but also to the children whom their cooperation with the police was meant to protect.

Until today, we have *never* held—or even suggested—that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain. Without so much as discussing the point, the Court today opens a hole in our Fourth Amendment jurisprudence, the size and shape of which is entirely indeterminate. Today's holding would be remarkable enough if the confidential relationship violated by the police conduct were at least one protected by state law. It would be surprising to learn, for example, that in a State which recognizes a spousal evidentiary privilege the police cannot use evidence obtained from a cooperating husband or wife.

There remains to be considered the first possible basis for invalidating this search, which is that the patients were coerced to produce their urine samples by their necessitous circumstances, to wit, their need for medical treatment of their pregnancy. If that was coercion,

it was not coercion applied by the government—and if such nongovernmental coercion sufficed, the police would never be permitted to use the ballistic evidence obtained from treatment of a patient with a bullet wound. And the Fourth Amendment would invalidate those many state laws that require physicians to report gunshot wounds, evidence of spousal abuse, and evidence of child abuse.

As I indicated at the outset, it is not the function of this Court—at least not in Fourth Amendment cases—to weigh petitioners' privacy interest against the State's interest in meeting the crisis of "crack babies" that developed in the late 1980's. I cannot refrain from observing, however, that the outcome of a wise weighing of those interests is by no means clear. The initial goal of the doctors and nurses who conducted cocaine testing in this case was to refer pregnant drug addicts to treatment centers, and to prepare for necessary treatment of their possibly affected children. When the doctors and nurses agreed to the program providing test results to the police, they did so because (in addition to the fact that child abuse was required by law to be reported) they wanted to use the sanction of arrest as a strong incentive for their addicted patients to undertake drug-addiction treatment. And the police themselves used it for that benign purpose, as is shown by the fact that only 30 of 253 women testing positive for cocaine were ever arrested, and only 2 of those prosecuted.

Notes

1. Many state laws require physicians to report if they detect particular injuries or patterns of behavior in the ordinary course of treatment. Such laws are applicable in cases of child abuse or neglect and intentional gun or knife wounds. What is so different about this case?
2. One major factor in the Court's view is the lack of voluntariness. Here, a person is pregnant. Medical treatment is only optional is the broadest sense of the term. In contrast, in one case on public employee drug testing, the Court noted several important limitations that added to the reasonableness of the search.[103] Only employees tentatively accepted for promotion for one of three specified categories of jobs were tested; applicants knew in advance that drug tests were a requirement for promotion; as in the student athlete case, there was no direct observation of the urination; and the test was for limited types of drugs.
3. In contrast, courts have been more skeptical in cases where the intrusion is severe. In the border search context, for instance, reasonable suspicion is required for more invasive searches, such as body cavity and strip searches.[104] But reasonable suspicion is not required for even extensive searches of non-private physical objects. In one case, the Supreme Court upheld a border search of a car's gas tank—which required substantial dismantling—on the grounds that it was not an especially private space when compared to a passenger compartment.[105]
4. Another major factor in these cases is the potential for arbitrary or abusive enforcement. The Court is wary of "standardless and unconstrained discretion" on the part of low-level government agents and prefers programs in which "the discretion of the official in the field be circumscribed, at least to some extent."[106] It is precisely to restrain such discretion that the warrant process involves a disinterested magistrate, who can shield citizens from

---

[103] *Nat'l Treasury Emps. Union*, 489 U.S. at 672 n.2.

[104] *See Tabbaa v. Chertoff*, 509 F.3d 89, 98 (2d Cir. 2007) (observing that strip and body cavity searches generally require reasonable suspicion); *United States v. Ramos-Saenz*, 36 F.3d 59, 61 (9th Cir. 1994) (concluding that strip and body cavity searches at the border go "beyond the routine"); *United States v. Johnson*, 991 F.2d 1287, 1292 (7th Cir. 1993) (noting that strip and body cavity searches are intrusive and "non routine").

[105] *United States v. Flores-Montano*, 541 U.S. 149, 154 (2004).

[106] *Delaware v. Prouse*, 440 U.S. 648, 661 (1979) (determining a checkpoint regime to be unreasonable).

potential abuse.[107] When the Court upheld the regulatory search of a firearms dealer, it specifically noted that "the possibilities of abuse and the threat to privacy are not of impressive dimensions," the scope of the inspection being determined in part by a specific statute.[108] This concern with unfettered discretion is in part what motivates Christopher Slobogin's call for greater *ex ante* legislative and administrative involvement in what he terms "panvasive" surveillance.[109] Given that the police are playing an effectively policy-making role, he would ask that the police follow the usual rules of administrative agencies when creating surveillance regimes.[110]

5. The Court also considers whether the enforcement regime is likely to work. In a drivers' license checkpoint case, it was skeptical that the described process would actually detect unlicensed drivers.[111] It therefore concluded that the spot checks were not "sufficiently productive to qualify as a reasonable law enforcement practice under the Fourth Amendment" even though the intrusion on individual drivers was "limited in magnitude."[112] The Court does not, however, insist that a policy be optimal. The choice among "reasonable alternatives remains with" the other branches of government.[113]
6. Some might read *Ferguson* and think that the presence of law enforcement alone is decisive. But consider the emergency aid exception. Under this exception, law enforcement officials may enter a home without a warrant to render aid to an occupant in peril. In *Case v. Montana*, 607 U.S. ___ (2026), the Supreme Court considered a case where police were dispatched to do "a welfare check on a suicidal male" in response to a call from the subject's exgirlfriend. Though entry into a home would normally require a warrant based upon probable cause, an emergency-aid entry requires only an "objectively reasonable basis" for believing that an occupant is injured or "faces serious danger." So the police were permitted entry here. The emergency aid exception is limited, however, and "provides no basis to search the premises beyond what is reasonably needed to deal with the emergency while maintaining the officers' safety."
7. Similarly, statutes requiring those charged or convicted of certain sex crimes to submit to HIV testing at the request of their alleged victim have also been upheld under the special needs doctrine.[114] Though the collection of a blood sample for an HIV test is undoubtedly a search, it has been held to be a reasonable one given the health concerns of the victim.

---

[107] *Camara v. Mun. Ct. of San Francisco*, 387 U.S. 523, 532–33 (1967) ("This is precisely the discretion to invade private property which we have consistently circumscribed by a requirement that a disinterested party warrant the need to search.").

[108] *United States v. Biswell*, 406 U.S. 311, 317 (1972) (upholding search and seizure in the context of a pawnshop selling firearms).

[109] Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 118–20 (2016).

[110] *Id.* at 120–22.

[111] *Prouse*, 440 U.S. at 660.

[112] *Id.* at 660–61.

[113] *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 453–54 (1990).

[114] See, e.g., *State in Int. of J.G.*, 289 N.J. Super. 575, 584 (1996) (both reaching that result and collecting cases). Such "testing, albeit not necessarily conclusive, will provide information to the victim of a sexual assault concerning the HIV status of his/her assailant at a point in time. Rightly or wrongly, the information may ease a victim's anxiety. The test results also serve the state's interest in safeguarding the health and safety of the offender and those with whom he/she comes in contact." *Id* at 592.

D. Wiretapping and the Electronic Communications Privacy Act

In addition to being regulated by the Fourth Amendment, government investigations are also subject to a variety of statutory restrictions. By far the most important of these is the Electronic Communications Privacy Act of 1986 (ECPA). This act is composed of three Titles:

Title I, which is often referred to as the Wiretap Act, prohibits any person from intercepting the content of live oral, wire, or electronic communications.

Title II, which is called the Stored Communications Act (SCA), protects the privacy of the contents of files stored by certain kinds of service providers.

Title III, the Pen Register Act, protects the privacy of non-content information against live interception.

Somewhat confusing, the Wiretap Act (Title I) was previously Title III of The Omnibus Crime Control and Safe Streets Act of 1968. So, you will occasionally see wiretap warrants referred to as "Title III" warrants even though the Wiretap Act is now in Title I. You have every right to be annoyed by this.

It may help to imagine this as a 2 x 2 table.

	Live interception	Access of stored records
Content information	Wiretap Act	Stored Communications Act
Non-content information/metadata	Pen Register Act	Stored Communications Act

The importance of the stored versus live distinction and of the content versus non-content distinction cannot be overstated. These distinctions put you under different statutes. Whenever you see the word "content" in this section, please consider it to be italicized. It is always important.

Both the government and major telecom companies provide statistics on information obtained under the ECPA and similar statutes. This data shows that importance of "wiretaps" has declined over the years. Consider the following table showing the kind of requests Verizon has received from the government in each semiannual period between 2019 and 2023:

Law Enforcement Demands for Customer Data – United States

	1H 2019	2H 2019	1H 2020	2H 2020	1H 2021*	2H 2021	1H 2022	2H 2022	1H 2023
Subpoenas	68,192	64,136	66,773	59,264	63,665	56,641	59,456	54,681	61,919
General Orders	19,269	12,586	5,760	4,062	3,841	3,485	3,809	3,400	3,539
Pen Register/ Trap & Traces	3,753	3,866	3,721	4,492	4,242	3,830	3,961	3,970	4,393
Wiretaps	585	525	612	627	415	387	313	286	382
Warrants	13,870	18,721	16,818	15,061	15,139	14,233	16,415	17,373	21,835
Emergency Requests From Law Enforcement	30,365	33,518	34,868	37,760	34,976	35,726	32,618	35,251	35, 698
Total	**136,034**	**133,352**	**128,552**	**121,266**	**122,278**	**114,302**	**116,572**	**114,961**	**127,766**

As should be readily apparent, actual wiretaps make up less than 400 of the almost 130,000 law enforcement requests Verizon received in the first half of 2023.[115] Though Verizon (and other cellular carriers) do not break this report down by exact statutory authority, you will see that the overwhelming majority of these requests come under the Stored Communications Act.

There are many reasons for this. Government actors will sometimes point out that the rise of end-to-end encryption makes live interception of message content—for example, in many standalone messaging apps—technologically impossible. Recall that a wiretap warrant gives the government legal permission to tap a conversation, not the magical ability to do so. But there is a more general issue. Live monitoring, as under the Wiretap Act, is prospective. It can only capture things that happen in the future. Stored records, on the other hand, extend into the past. If you are investigating a crime that happened last month, there is an obvious advantage to being able to rewind the clock and look at records from the time of the offense itself. In a world where there are a lot of these past records, they serve as an extremely attractive target for government investigators.

1) The Wiretap Act

Each of these Titles revolves heavily around a series of definitions. Not all communications are protected from interception by the Wiretap Act and not all service providers are covered by the SCA. Consider the primary operative provision of the Wiretap Act, 18 U.S.C § 2511:

[115] Verizon publishes these transparency reports every six months at https://www.verizon.com/about/investors/transparency-report.

(1) Except as otherwise specifically provided in this chapter any person who—

> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> (b) intentionally uses . . . any electronic, mechanical, or other device to intercept any oral communication . . . ;
>
> (c) intentionally discloses, . . . the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained . . . in violation of this subsection;
>
> (d) intentionally uses . . . the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained . . . in violation of this subsection . . .

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

So, the Wiretap Act applies to wire, oral, and electronic communications. These are defined terms under 18 U.S.C. § 2510:

> (1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection . . . furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;
>
> (2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;
>
> (12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include [any wire or oral communication].

Since "aural transfer" means a transmission "containing the human voice," telephone calls and Zoom meeting are wire communications. A fax is not, however, because it does not involve the human voice. A private conversation in an empty park is an oral communication, but the same conversation on a busy train platform is not; the speakers have no reasonable expectation that others will not overhear in a crowded space. An email would be an electronic communication, as would a live feed from a video-only camera and a fax.

After defining these terms, the act then prohibits a person from seeking to "intercept" any of these forms of communication. Intercept means to acquire the *contents* of (any of the above) "through the use of any electronic, mechanical, or other device." So merely eavesdropping

is fine. Using a device to overhear another person is not.[116] Further, the interception must be live, meaning contemporaneous. If I hack into your video call and covertly record it, I have violated the Wiretap Act. If I hack into your computer and steal a recording you yourself made of your video call then I have violated several other laws, but not the Wiretap Act.[117]

This brings us to the exceptions. Certain interceptions are permissible. Most basically, the consent of any one party to the communication functions as a defense. So, if Person A is speaking with Person B, Person C can record their conversation with Person A's permission. This is true even if Person B is not aware of the recording.

There is also an exception that permits an employee or agent of a communications service to intercept, disclose, and use communications "while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2511(2)(a)(i). Further, the service provider may disclose to law enforcement content which was "inadvertently obtained by the service provider and which appear to pertain to the commission of a crime." § 2511(3)(b)(iv).

The Wiretap Act prohibits interception both by private parties as well as by the government. In the case of private parties, a violation of the Wiretap Act is both a civil wrong—punishable by substantial monetary damages—as well as a crime.

a) Interception by the government

Since the Wiretap Act prohibits government interception generally, it needs to address when interception should be permissible. There are two main circumstances in which the government is allowed to intercept wire, oral, and electronic communications. The first is through the issuance of what is generally called a "super warrant."

A super warrant differs from a traditional warrant in several important ways:

- Only a select number of federal officials can apply for such a warrant, rather than every prosecutor.[118]
- Such warrants can only be issued when the interception is expected to provide evidence of a serious crime, generally meaning an offense punishable by at least one year imprisonment or death.[119] 18 U.S.C. § 2516(1). The statute also specifically imposes limits on state wiretaps, with again a restricted list of officers being allowed to apply for a wiretap warrant and a specific—and more limited—set of qualifying crimes. § 2516(2)–(3).
- Other investigative procedures must have been tried and failed or appear unlikely to be successful. § 2518(3)(c).

---

[116] The statute specifically exempts hearing aids 18 U.S.C. § 2510(5(b), which gives you a sense of how broad it is otherwise. There is even a provision stating that it is permissible to intercept broadcasts to the general public and signals made accessible to the general public. 18 U.S.C. § 2511(2)(g).

[117] This turns out to be both difficult and important in the context of email. *See, e.g.*, *United States v. Szymuszkiewicz*, 622 F.3d 701, 704 (7th Cir. 2010), as amended (Nov. 29, 2010) (considering the details of an email forwarding program's function before concluding that it was sufficiently contemporaneous to lead to liability under the Wiretap Act rather than the Stored Communications Act).

Also, this is yet another occasion to flag the "violates several laws but not this one" problem in privacy law. Beware the client, reporter, or student who is too focused on whether a particular statute applies to a given set of facts. There are a lot of statutes out there. It is much easier to say that something is illegal than to say that it is legal.

[118] Specifically, "The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General." 18 U.S.C. 2516 (1).

[119] The list of included offenses extends from 1(a)-1(u).

- The interception of non-covered communications must be minimized. § 2518(5).
- There are also heightened particularity requirements, specifying exactly when the interception will occur and for how long, who will be doing the monitoring, etc.

Most important here are the limited number of officials who can apply for a warrant; the requirement that other means have been exhausted; and the heightened particularity standard. In other words, the application is long and your boss's boss must sign off on it.

The second major way such interception can be legal is with an order under the Foreign Intelligence Surveillance Act (FISA). That is addressed in Chapter 4. I mentioned it here because students are sometimes confused about the relationship between these two statutes. They are independent ways to make the interception of various forms of communication legal.

There is also an emergency interception provision, § 2518(7), which permits a wiretap in cases of immediate danger, threats to national security, and similar. In such cases, the authorizing official needs to apply for the warrant retrospectively. If the warrant is denied, the interception is treated as if it were illegal.

b) Interception by private actors and penalties

The Wiretap Act also applies to private parties and can be enforced by private parties.

> "[A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity . . . ." 18 U.S.C § 2520.

Violations of this can result in civil damages, including punitive damages, equitable relief, and attorney fees. Key from a civil litigation standpoint, the act has a statutory damages provision:

> (2) In any other action under this section, the court may assess as damages whichever is the greater of—
>
> (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or
>
> (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

Consider how this would play out in a civil case. You tap your spouse's phone. You discover they are having an affair and file for a divorce, citing the recordings. Or your boss records your phone calls without your permission and seeks to fire you based on poor performance displayed in the recordings. In each case, the monitored party has a valid and expensive cause of action despite their potential misconduct. You also see class actions based on monitoring by technology companies, in which the daily damages are quite extensive.

c) Exclusionary rule

Under 18 U.S.C. § 2515, "Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding." Notably this provision does not mention *electronic* communication, which do not enjoy exclusionary rule protection under the Wiretap Act itself. Courts may exclude such evidence anyway, but the statute does not specifically require it.

Further, do recall the interaction between the Wiretap Act and the Fourth Amendment. Where a statute disagrees with the constitution, the constitution controls. So if, under *Warshak*, the Fourth Amendment requires the exclusion of emails illegally obtained by the government, then the lack of statutory exclusion in the Wiretap Act does not override that.

Notes

1. Only the contemporaneous or "live" interception of content material is covered by the Wiretap Act. Access to stored content material is covered by the less-protective SCA. The New Jersey Supreme Court recently examined what counted as contemporaneous interception in the context of Facebook messages. The state had argued that the interception of the Facebook user's prospective (future) communications was not contemporaneous because Facebook could only generate a report for them every fifteen minutes, meaning they would be stored by the time they were actually produced to the government. *Facebook, Inc. v. State*, 296 A.3d 492, 510 (2023). Thus, the messages would necessarily be at least a few minutes stale. The court held that the near-contemporaneous collection of communications was still "live" enough to fall within the scope of the state wiretap act. Therefore, a wiretap warrant, rather than lesser process, was needed.
2. Note the caption in the above case: *Facebook v State*. Due to the way in which these requests are served—from the government to a technology company—the actual criminal suspect is usually not involved in the initial phase of the litigation. Instead, those whom the government seeks to investigate are generally forced to rely on the technology companies to assert their rights for them, at least in the first instance. In the event that the information was unlawfully produced, the suspect could later litigate the evidence's admissibility at a suppression hearing.

2) State Wiretap Law

One of the most important features of state wiretap law is that it varies by state. An interception that is legal in one state can easily be illegal in another. Consider the example of Illinois' statute, 720 ILCS 5/14-2. The statute defines the term "private conversation":

> For the purposes of this Article, "private conversation" means any oral communication between 2 or more persons, whether in person or transmitted between the parties by wire or other means, when one or more of the parties intended the communication to be of a private nature under circumstances reasonably justifying that expectation . . . .

Broadly speaking, this mirrors the federal definition of oral communication. The Illinois statute then establishes a basic rule for the offense:

> (a) A person commits eavesdropping when he or she knowingly and intentionally:
>
> > (1) Uses an eavesdropping device, in a surreptitious manner, for the purpose of overhearing, transmitting, or recording all or any part of any private conversation to which he or she is not a party unless he or she does so with the consent of all of the parties to the private conversation;
> >
> > (2) Uses an eavesdropping device, in a surreptitious manner, for the purpose of transmitting or recording all or any part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation;
> >
> > (3) Intercepts, records, or transcribes, in a surreptitious manner, any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication;

The statute then lists the exceptions and affirmative defenses. A variety of uses by law enforcement, or to monitor law enforcement, are specifically mentioned. For instance, in 5/14-3(e):

> Nothing in this Article shall prohibit any individual, not a law enforcement officer, from recording a law enforcement officer in the performance of his or her duties in a public place or in circumstances in which the officer has no reasonable expectation of privacy. However, an officer may take reasonable action to maintain safety and control, secure crime scenes and accident sites, protect the integrity and confidentiality of investigations, and protect the public safety and order.

The other exemptions range down to (q). There is much to note here. Most basically, the statute is an all-party consent statute. Regardless of whether you are in the conversation, you cannot monitor the conversation without the consent of all parties. This is a sharp difference from the federal law, which requires only the consent of a single participant. Also, this is specifically a ban on surreptitious recording. Obvious or announced recording is therefore always permissible. So simply telling a person "This call is recorded" makes recording the call legal. In addition to not being surreptitious monitoring, this statement would also likely defeat treating the interaction as a "private conversation" under the state definition. Eavesdropping is a felony in Illinois, and evidence illegally obtained by eavesdropping is not admissible in court.

The single largest difference between states in their wiretapping laws is whether they are all-party consent or one-party consent. Of the fifty states and the District of Columbia, Puerto Rico, and Guam, thirty-seven states permit audio recordings with one party's consent, twelve require all parties to consent, three have mixed laws, and one state (Vermont) does not specify. But there are also nuances in their exceptions. In Connecticut, all parties are required to consent to avoid civil liability, but verbal notification prior to the start of the recording can suffice. CONN. GEN. STAT. § 52-570d. And recall the exception in Illinois that specifically allows for the recording of the police.

3) The Pen Register Act

The pen register statute is the non-content counterpart to the federal Wiretap Act and serves as a legislative response to *Smith v. Maryland*. The procedural protections offered under the pen register statute pale in comparison to those of the Wiretap Act. First, any government attorney may apply for a pen register order. 18 U.S.C. § 3122(a)(1). Second, that attorney must include "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." § 3122 (b)(2). Two important points here. First, the attorney is certifying, meaning claiming. They are not providing a detailed basis for their certification. Second, they are certifying that the information will be *relevant* to an ongoing criminal investigation. Relevancy is a low bar.

Under the pen register statute, the government may not install a pen register or trap-and-trace device without the kind of court order described above. The key to understanding this statute are the definitions found in § 3127 of those two devices:

> (3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

> (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

Two important notes regarding this pair of definitions. First, they are broadly written to capture all non-content data conveyed across a computer or telephone network. It is well within this legal definition for a pen register to monitor which websites a computer visits. The definitions explicitly exclude content data, however. This marks the border between the Wiretap Act (content) and the Pen Register Act (non-content). Second, these definitions concern ongoing or live interception of traffic. This is the interception of signals in transit, not records of signals. That is the boundary between the Pen Register Act and portions of the Stored Communications Act, which takes the opposite approach.

The Pen Register statute also does not provide for an exclusionary remedy. It is a crime to install a pen register or trap-and-trace device without authorization, however. § 3127(d).

4) The Stored Communications Act

The SCA is substantially more complicated than the Wiretap Act. It regulates the protection of data held by two particular kinds of entities: Remote Computing Services (RCS) and Electronic Communications Services (ECS). An entity might be an ECS, an RCS, both, or neither. If it is neither, then the SCA does not apply to it and records held by the company are only protected by the Fourth Amendment.

To understand the meaning of ECS and RCS, it is helpful to consider the state of computer technology at the time in which the statute was passed. As the 1986 Senate Report on the SCA explains, computer network account holders at that time generally used third-party network service providers in two ways. First, account holders used their accounts to send and receive communications such as email. The provider of such a service would hold in its own storage a copy of the record. This copy might be comparatively ephemeral—held only until delivery—or stored for a longer period.

The second reason account holders used network service providers was to outsource computing tasks. For example, users paid to have remote computers store extra files or process large amounts of data. This is the precursor of modern cloud providers today, though the tasks then at issue are far below what is done locally on laptops now. When users hired such commercial "remote computing services" to perform tasks for them, they would send a copy of their private information to a third-party computing service, which retained the data for storage or processing. This leads to the three key definitions of the SCA:

> "Electronic communication service" (ECS) means any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15).

Protection is provided to information that an ECS holds in "electronic storage." 18 U.S.C. § 2701(a)(2).

> "electronic storage" means—
>
> > (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
> >
> > (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

Further, protections are also offered to data held by remote computing services. 18 U.S.C. § 2702(a)(2).

> "Remote computing service" (RCS) means the provision to the public of computer storage or processing services by means of an electronic communications system. 18 U.S.C. § 2711(2).

It is often challenging to determine whether an entity is operating as an RCS or ECS for a given set of data. There is, for example, currently a complex legal morass about the status of opened email messages stored in a user's email account. Such an email is not held in electronic storage in the sense that the storage is incidental to transmission. It may be in electronic storage in the sense that it is a "backup" copy. *Hately v. Watts*, 917 F.3d 770, 794–795 (4th Cir. 2019). But if it is not, then the email is now only granted RCS protections. Unopened email, however, is certainly held incident to transmission and will get ECS protection.

RCS is broader than it may initially appear because of the definition of electronic communications system: "any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14). This effectively means that Google Drive and Dropbox are RCS. The main challenge with RCS is the "provision to the public" language. If your university provides you network drive storage because you are a student or faculty member, that is not "provision to the public," meaning that the university if not functioning as an RCS for the purposes of that drive.

a) Required disclosures under 18 U.S.C § 2703

Depending on whether a provider is functioning as an ECS or RCS for the purposes of a given set of data, and depending on what the data is, the government needs to produce different levels of legal process to force the data's disclosure. The general rule here is that the government can always use greater process than is required. So, if the statute requires a subpoena, the government can always get a full search warrant. It is most helpful to start at the bottom of the chain and work up:

With a simple subpoena, the government can compel basic subscriber information from either an RCS or ECS. This would include the subscriber's name, address, session logs (call duration type information), telephone number, assigned IP address, and means of payment.

With a § 2703(d) order, sometimes called just a (d) order, the government can compel more. To obtain a (d) order, the government must present "specific and articulable facts showing that there are reasonable grounds to believe" that the information will be "relevant and material to an ongoing investigation." This is not an especially demanding standard. Such an order allows the government to compel the production of all non-content records.

With prior notice to the subscriber, a subpoena or a § 2703(d) order, it can compel the production of the contents of a RCS. Notice can be delayed under § 2705 if giving notice would do any of several things, such as endanger the life or safety of an individual, allow for the destruction of evidence, or otherwise seriously interfere with an investigation.

A search warrant (recall the probable cause standard) can compel the production of all account information, including unopened email. A warrant is the only way to compel the production of unopened email in storage for 180 days or less. One historical oddity of the statute is that it treats unopened email in storage for more than 180 days as entitled to lesser protection, producible with only a subpoena or § 2703(d) order, as with RCS content information.

Considering *Warshak*, it is clear that the SCA is providing less protection than is constitutionally necessary to at least some of these categories of data. Specifically, email

content—however long in storage—requires a warrant to produce. To the extent the SCA states otherwise, it is unenforceable. The important provisions of the SCA are therefore those that provide more protection than does the Fourth Amendment: those provisions that require some legal process for non-content information, which would generally not be protected at all under *Smith*.

b) Limits on voluntary disclosure under 18 U.S.C § 2702

As § 2703 requires disclosures to the government in a host of cases, § 2702 prohibits disclosures to both the government and private parties in a host of cases. To begin, any ECS or RCS that provides "service to the public" is banned from disclosing subscriber content information unless otherwise authorized (for example, by § 2703).[120] It then gives a series of exceptions permitting disclosure:

- To the subscriber or with their consent;
- As needed to administer the service, for example to actually deliver the electronic communication;
- To make a report to the National Center of Missing and Exploited Children under § 2258A;
- To a law enforcement agency if the contents were inadvertently obtained and appear to pertain to the commission of a crime;
- To the government, when death or risk of serious injury is imminent and urgent action is needed.

All the above exceptions concern disclosure of subscriber content information. There are similar exceptions allowing for the disclosure of subscriber noncontent information, or "customer records." But there is one important additional exception allowing for the disclosure of noncontent information. It can be disclosed "to any person other than a governmental entity" § 2702(c)(6).

Consider the importance of this additional exception for non-content information. This means that a company can mine metadata and sell it despite the protections provided by the SCA to content data.

c) Penalties

Any person aggrieved by a knowing or intentional violation of the SCA can bring a civil action under § 2707(a). In a key difference from the Wiretap Act, courts may assess "actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000." § 2707(c). These damages are much lower than the statutory damages available under the Wiretap Act, though punitive damages are still available if the conduct is willful. It is possible to bring a civil action against the United States, but there are a host of requirements and limitations. § 2712.

There is not a statutory exclusion remedy for violations of the SCA.

Notes

1. The possibility of statutory civil damages has proven appealing to some plaintiff-side attorneys. Several lawsuits, however, have been defeated on the grounds that the sued party is outside the scope of the SCA. The judge deciding *In re JetBlue Airways Corp. Priv. Litig.*, 379 F.Supp.2d 299, 307 (E.D.N.Y. 2005) held that "a company such as JetBlue does not become an 'electronic communication service' provider simply because it maintains a

[120] Disclosure to a foreign law government in response to a foreign order is allowed under limited circumstanced. § 2702(b)(9).

website that allows for the transmission of electronic communications between itself and its customers." Similarly, JetBlue is not a remote computing service because "no facts alleged indicate that JetBlue provides either computer processing services or computer storage to the public." Similarly, Amazon was able to dismiss an SCA claim over Siri because it too was not an ECS. *Garner v. Amazon.com, Inc.*, 603 F.Supp.3d 985, 1003–04 (W.D. Wash. 2022) ("A company that merely utilizes electronic communications in the conduct of its own business is generally considered a purchaser or user of the communications platform, not the provider of the service to the public.").

2. Facebook, by contrast, has been held to be an ECS for its messaging functions and an RCS for private posts on a Facebook wall. *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965, 980, 990 (C.D. Cal. 2010). But this is a highly context-specific decision. In the context of private postings, Facebook is effectively storing data. In the context of private messaging, Facebook is effectively functioning as an email/text messaging equivalent. In other contexts, however, Facebook is doing neither of those things. For this reason, a court held that LinkedIn was not an ECS or RCS with respect to a particular set of cookie and targeted-advertising practices. *Low v. LinkedIn Corp.*, 900 F.Supp.2d 1010, 1023 (N.D. Cal. 2012). Presumably the court would have come to a different conclusion if it had been asked to assess the status of LinkedIn's private messaging function.

IV. National Security

A. Overall framework 217
U.S. v. U.S. Dist. Court for Eastern Dist. of Mich., 407 U.S. 297 (1972) [The Keith Case] 218

B. Foreign Intelligence Surveillance Act 224
In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) 225
United States v. Aziz, 228 F.Supp.3d 363 (M.D. Penn. 2017) 235

C. National Security Letters 237
1) Types of National Security Letters 238
2) Constitutionality of Gag Orders 240

D. Section 215 and the metadata program 240
United States v. Moalin 973 F.3d 977 (9th Cir. 2020) 241

E. Section 702 and surveillance overseas 248
Clapper v. Amnesty Intern. USA, 568 U.S. 398 (2013) 249
United States v. Muhtorov, 20 F.4th 558 (10th Cir. 2021) 257

National security involves a range of agencies, statutes, and doctrinal concerns far different from those already reviewed. The targets of surveillance are different than they are in the traditional criminal context, how targets are surveilled is different, and the people doing the surveillance are different. This chapter introduces both new statutory frameworks – most notably the Foreign Intelligence Surveillance Act – as well as new constitutional considerations. In particular, courts have long struggled to determine when and how the national security context influences Fourth Amendment analysis.

A. Overall framework

The first question we must face is a simple one: are we in the realm of national security? Do the normal rules of criminal investigations apply, or is this a national security matter, and therefore, a special case?

The seminal case on this topic is known as the Keith case. It is named for District Court Judge Damon Keith. In a pretrial motion, Judge Keith had held that the government needed to disclose the contents of certain wiretap evidence to the defense. The government then filed a writ of mandamus challenging the decision. The Sixth Circuit rejected the government's argument, and the Supreme Court granted cert. The actual case citation is both nondescriptive and hard to abbreviate, hence the use of Keith's name in its place.

The underlying case was a criminal prosecution of three individuals for their alleged roles in three bombings in Ann Arbor, Michigan that took place in 1968. These bombings targeted a covert CIA office, the entryway of a campus building conducting scientific research (including potentially some military research), and a car outside the campus ROTC building. No one was injured in any of the bombings

The defendants in the case were leaders of the radical White Panther party, which was a white antiracist group formed in solidarity with the Black Panthers. Their political platform called for free education, the abolition of money, and the end of "political oppression of the

people by the vicious pig power structure and their mad dog lackies the police, courts, and military."[121]

The FBI's case against the trio included recorded conversations from a phone wiretapped for an unrelated investigation. The wiretap was conducted without a warrant and the key question before the Supreme Court was whether this warrantless surveillance was legal given that it was aimed at a group suspected of attempting to overthrow the United States government.

U.S. v. U.S. Dist. Court for Eastern Dist. of Mich., 407 U.S. 297 (1972) [The Keith Case]

Mr. Justice POWELL delivered the opinion of the Court.

The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power . . . to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time.

This case arises from a criminal proceeding in the United States District Court for the Eastern District of Michigan, in which the United States charged three defendants with conspiracy to destroy Government property . . . . One of the defendants, Plamondon, was charged with the dynamite bombing of an office of the Central Intelligence Agency in Ann Arbor, Michigan.

Title III of the Omnibus Crime Control and Safe Streets Act authorizes the use of electronic surveillance for classes of crimes carefully specified in 18 U.S.C. § 2516. Such surveillance is subject to prior court order. Section 2518 sets forth the detailed and particularized application necessary to obtain such an order as well as carefully circumscribed conditions for its use. The Act represents a comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression. Much of Title III was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court in *Berger v. New York* (1967), and *Katz v. United States* (1967).

Together with the elaborate surveillance requirements in Title III, there is the following proviso, 18 U.S.C. § 2511(3):

> 'Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.'

The Government relies on § 2511(3). It argues that 'in excepting national security surveillances from the Act's warrant requirement Congress recognized the President's authority to conduct such surveillances without prior judicial approval.' The section thus is

---

[121] John Sinclair, *White Panther Party 10-Point Program*, SUN: FREE NEWSPAPER OF DOPE, ROCK 'N' ROLL AND FUCKING IN THE STREETS! RIGHT ON!, July 28, 1969, https://media.aadl.org/documents/pdf/aa_sun/aa_sun_19690728.pdf.

viewed as a recognition or affirmance of a constitutional authority in the President to conduct warrantless domestic security surveillance such as that involved in this case.

We think the language of § 2511(3), as well as the legislative history of the statute, refutes this interpretation. The relevant language is that: 'Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect . . .' [a]gainst the dangers specified. At most, this is an implicit recognition that the President does have certain powers in the specified areas. Few would doubt this, as the section refers—among other things—to protection 'against actual or potential attack or other hostile acts of a foreign power.' But so far as the use of the President's electronic surveillance power is concerned, the language is essentially neutral.

The express grant of authority to conduct surveillances is found in § 2516, which authorizes the Attorney General to make application to a federal judge when surveillance may provide evidence of certain offenses. These offenses are described with meticulous care and specificity.

In view of these and other interrelated provisions delineating permissible interceptions of particular criminal activity upon carefully specified conditions, it would have been incongruous for Congress to have legislated with respect to the important and complex area of national security in a single brief and nebulous paragraph. This would not comport with the sensitivity of the problem involved or with the extraordinary care Congress exercised in drafting other sections of the Act. We therefore think the conclusion inescapable that Congress only intended to make clear that the Act simply did not legislate with respect to national security surveillances.

[V]iewing § 2511(3) as a congressional disclaimer and expression of neutrality, we hold that the statute is not the measure of the executive authority asserted in this case. Rather, we must look to the constitutional powers of the President.

It is important at the outset to emphasize the limited nature of the question before the Court. This case raises no constitutional challenge to electronic surveillance as specifically authorized by Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Nor is there any question or doubt as to the necessity of obtaining a warrant in the surveillance of crimes unrelated to the national security interest. Further, the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country. The Attorney General's affidavit in this case states that the surveillances were 'deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of Government' (emphasis supplied). There is no evidence of any involvement, directly or indirectly, of a foreign power.

Our present inquiry, though important, is therefore a narrow one. It addresses a question left open by *Katz*:

> 'Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security . . . .'

We begin the inquiry by noting that the President of the United States has the fundamental duty, under Art. II, § 1, of the Constitution, to 'preserve, protect and defend the Constitution of the United States.' Implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means. In the discharge of this duty, the President—through the Attorney General—may find it necessary to employ electronic surveillance to obtain intelligence information on the plans of those who plot unlawful acts against the Government. The use of such surveillance in internal security cases has been sanctioned more or less continuously by various Presidents and Attorneys General since July 1946. Herbert Brownell, Attorney General under President Eisenhower, urged the use of

electronic surveillance both in internal and international security matters on the grounds that those acting against the Government

> 'turn to the telephone to carry on their intrigue. The success of their plans frequently rests upon piecing together shreds of information received from many sources and many nests. The participants in the conspiracy are often dispersed and stationed in various strategic positions in government and industry throughout the country.'

Though the Government and respondents debate their seriousness and magnitude, threats and acts of sabotage against the Government exist in sufficient number to justify investigative powers with respect to them.[12] The covertness and complexity of potential unlawful conduct against the Government and the necessary dependency of many conspirators upon the telephone make electronic surveillance an effective investigatory instrument in certain circumstances. The marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission, and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its law-abiding citizens.

But a recognition of these elementary truths does not make the employment by Government of electronic surveillance a welcome development—even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens.[13] We look to the Bill of Rights to safeguard this privacy. Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance.

National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. 'Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power,' *Marcus v. Search Warrants etc.* (1961). History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent. Senator Hart addressed this dilemma in the floor debate on § 2511(3):

> 'As I read it—and this is my fear—we are saying that the President, on his motion, could declare—name your favorite poison—draft dodgers, Black

---

[12] The Government asserts that there were 1,562 bombing incidents in the United States from January 1, 1971, to July 1, 1971, most of which involved Government related facilities. Respondents dispute these statistics as incorporating many frivolous incidents as well as bombings against nongovernmental facilities. The precise level of this activity, however, is not relevant to the disposition of this case.

[13] Professor Alan Westin has written on the likely course of future conflict between the value of privacy and the 'new technology' of law enforcement. Much of the book details techniques of physical and electronic surveillance and such possible threats to personal privacy as psychological and personality testing and electronic information storage and retrieval. Not all of the contemporary threats to privacy emanated directly from the pressures of crime control. *Privacy and Freedom* (1967).

> Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure or existence of the Government.'

The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.

As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression. If the legitimate need of Government to safeguard domestic security requires the use of electronic surveillance, the question is whether the needs of citizens for privacy and the free expression may not be better protected by requiring a warrant before such surveillance is undertaken. We must also ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it.

These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.

It may well be that, in the instant case, the Government's surveillance of Plamondon's conversations was a reasonable one which readily would have gained prior judicial approval. But this Court 'has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end.' The Fourth Amendment contemplates a prior judicial judgment,[18] not the risk that executive discretion may be reasonably exercised. This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government. The independent check upon executive discretion is not satisfied, as the Government argues, by 'extremely limited' post-surveillance judicial review. Indeed, post-surveillance review would never reach the surveillances which failed to result in prosecutions. Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights.

The Government argues that the special circumstances applicable to domestic security surveillances necessitate a further exception to the warrant requirement. It is urged that the requirement of prior judicial review would obstruct the President in the discharge of his constitutional duty to protect domestic security. We are told further that these surveillances are directed primarily to the collecting and maintaining of intelligence with respect to subversive forces, and are not an attempt to gather evidence for specific criminal prosecutions. It is said that this type of surveillance should not be subject to traditional warrant requirements which were established to govern investigation of criminal activity, not ongoing intelligence gathering.

---

[18] We use the word 'judicial' to connote the traditional Fourth Amendment requirement of a neutral and detached magistrate.

The Government further insists that courts 'as a practical matter would have neither the knowledge nor the techniques necessary to determine whether there was probable cause to believe that surveillance was necessary to protect national security.' These security problems, the Government contends, involve 'a large number of complex and subtle factors' beyond the competence of courts to evaluate.

As a final reason for exemption from a warrant requirement, the Government believes that disclosure to a magistrate of all or even a significant portion of the information involved in domestic security surveillances 'would create serious potential dangers to the national security and to the lives of informants and agents . . . . Secrecy is the essential ingredient in intelligence gathering; requiring prior judicial authorization would create a greater 'danger of leaks . . ., because in addition to the judge, you have the clerk, the stenographer and some other officer like a law assistant or bailiff who may be apprised of the nature' of the surveillance.'

These contentions on behalf of a complete exemption from the warrant requirement, when urged on behalf of the President and the national security in its domestic implications, merit the most careful consideration. We certainly do not reject them lightly, especially at a time of worldwide ferment and when civil disorders in this country are more prevalent than in the less turbulent periods of our history. There is, no doubt, pragmatic force to the Government's position.

But we do not think a case has been made for the requested departure from Fourth Amendment standards. The circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.

We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases. Certainly courts can recognize that domestic security surveillance involves different considerations from the surveillance of 'ordinary crime.' If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.

Nor do we believe prior judicial approval will fracture the secrecy essential to official intelligence gathering. The investigation of criminal activity has long involved imparting sensitive information to judicial officers who have respected the confidentialities involved. Judges may be counted upon to be especially conscious of security requirements in national security cases. Title III of the Omnibus Crime Control and Safe Streets Act already has imposed this responsibility on the judiciary in connection with such crimes as espionage, sabotage, and treason, each of which may involve domestic as well as foreign security threats. Moreover, a warrant application involves no public or adversary proceedings: it is an *ex parte* request before a magistrate or judge. Whatever security dangers clerical and secretarial personnel may pose can be minimized by proper administrative measures, possibly to the point of allowing the Government itself to provide the necessary clerical assistance.

Thus, we conclude that the Government's concerns do not justify departure in this case from the customary Fourth Amendment requirement of judicial approval prior to initiation of

a search or surveillance. Although some added burden will be imposed upon the Attorney General, this inconvenience is justified in a free society to protect constitutional values. Nor do we think the Government's domestic surveillance powers will be impaired to any significant degree. A prior warrant establishes presumptive validity of the surveillance and will minimize the burden of justification in post-surveillance judicial review. By no means of least importance will be the reassurance of the public generally that indiscriminate wiretapping and bugging of law-abiding citizens cannot occur.

We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents.

Moreover, we do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.' The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

Given those potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.

We do not attempt to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. We do hold, however, that prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.

Mr. Justice DOUGLAS, concurring.

Other abuses, such as the search incident to arrest, have been partly deterred by the threat of damage actions against offending officers, the risk of adverse publicity or the possibility of reform through the political process. These latter safeguards, however, are ineffective against lawless wiretapping and 'bugging' of which their victims are totally unaware.

We are told that one national security wiretap lasted for 14 months and monitored over 900 conversations. Senator Edward Kennedy found recently that 'warrantless devices accounted for an average of 78 to 209 days of listening per device, as compared with a 13-day per device average for those devices installed under court order.' He concluded that the Government's revelations posed 'the frightening possibility that the conversations of untold thousands of citizens of this country are being monitored on secret devices which no judge has authorized and which may remain in operation for months and perhaps years at a time.'

Such gross invasions of privacy epitomize the very evil to which the Warrant Clause was directed. This Court has been the unfortunate witness to the hazards of police intrusions which did not receive prior sanction by independent magistrates.

That 'domestic security' is said to be involved here does not draw this case outside the mainstream of Fourth Amendment law. Rather, the recurring desire of reigning officials to employ dragnet techniques to intimidate their critics lies at the core of that prohibition. For it was such excesses as the use of general warrants and the writs of assistance that led to the ratification of the Fourth Amendment.

Notes

1. The Keith Case can be read as creating a three-part framework for electronic surveillance.
    a. Ordinary criminal law enforcement requires a warrant (the holding of *Katz*), and is regulated under what is now the ECPA.
    b. Domestic intelligence gathering requires prior judicial approval (the holding of *Keith*), but Congress could create a legislative framework other than the ECPA to regulate it.
    c. Foreign intelligence gathering, including intelligence gathering overseas and intelligence gathering in the United States of agents of a foreign power, was left unaddressed in *Keith*.
2. Dissident political leaders are threats to the current political establishment; that is their role. It can be assumed that the current political establishment will not like them, will sometimes fear them, and will often be biased against them. This is why the Supreme Court is skeptical of letting the executive branch be the sole judge of when political dissent crosses the line and becomes a domestic security threat. Around the time of *Keith,* there were a series of revelations involving excesses of the FBI, CIA, NSA, and IRS in the monitoring of political dissidents. These ultimately led to the Church Committee being formed in 1975 to investigate all of these agencies. Among the programs reviewed by the Church Committee was the FBI's Counterintelligence Program (COINTELPRO), which infiltrated domestic groups that the FBI deemed subversive. These groups included the KKK, the Socialist Workers Party, the Black Panther Party, the Southern Christian Leadership Conference, and the Communist Party of the United States. The program included extensive surveillance of Dr. Martin Luther King Jr., as well as a broad network of Black nationalist and civil rights organizations. COINTELPRO was ultimately exposed when a radical group burgled an FBI office in 1971 and gave classified files describing the program to the media.
3. How clear is the line between domestic intelligence gathering and foreign intelligence gathering? Domestic political movements often have foreign connections, and the ease of international travel and communications in the present era may blur lines further. Imagine Dr. King had traveled to the Soviet Union and regularly corresponded with Soviet officials (in actuality, he did not).[122] Would that be sufficient to move surveillance of him from domestic intelligence gathering to foreign intelligence gathering?

B. Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act (FISA) is the national security counterpart of the ECPA. As currently written, it allows for electronic monitoring of foreign powers and agents of foreign powers who are operating in the United States so long as a significant purpose of the monitoring is to gather foreign intelligence information. This portion of the chapter considers FISA as it has traditionally functioned—as a means of surveilling people within the United States who are foreign powers or agents of foreign powers. Section 702 of FISA, which involves

[122] Foreign countries often have considerable interest in domestic political movements. The Soviet Union was broadly in favor of the American civil rights movement because of the propaganda value of the injustices it exposed. It also was broadly in favor of the anti-war movement because it wanted to win the war in Vietnam. King was part of both movements, but also resolutely anti-Communist despite his concerns with capitalism.

using American access to communication infrastructure to conduct surveillance overseas, will be considered separately.

To begin, let us consider the question of scope. When is an investigation sufficiently directed to a foreign intelligence goal? This question builds directly from the issues raised by *Keith*.

The below proceeding is an appeal from a decision of the Foreign Intelligence Surveillance Court (FISC). FISC is a court established by FISA to review FISA warrant applications. It consists of eleven Article III judges selected by the Chief Justice of the Supreme Court. Warrant denials by a FISC judge are reviewable by the Foreign Intelligence Surveillance Court of Review, which consists of three judges similarly appointed by the Chief Justice. This appellate court issued its first decision in 2002.[123]

In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002)

PER CURIAM

This is the first appeal from the Foreign Intelligence Surveillance Court to the Court of Review since the passage of the Foreign Intelligence Surveillance Act (FISA) in 1978. The appeal is brought by the United States from a FISA court surveillance order which imposed certain restrictions on the government. Since the government is the only party to FISA proceedings, we have accepted briefs filed by the American Civil Liberties Union (ACLU) and the National Association of Criminal Defense Lawyers (NACDL) as *amici curiae*.

After a careful review of the briefs filed by the government and *amici,* we conclude that FISA, as amended by the Patriot Act, supports the government's position, and that the restrictions imposed by the FISA court are not required by FISA or the Constitution.

The court's decision from which the government appeals imposed certain requirements and limitations accompanying an order authorizing electronic surveillance of an "agent of a foreign power" as defined in FISA. The FISA court authorized the surveillance, but imposed certain restrictions, which the government contends are neither mandated nor authorized by FISA. Particularly, the court ordered that law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division [of the Department of Justice] shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives.

To ensure the Justice Department followed these strictures the court also fashioned what the government refers to as a "chaperone requirement"; that a unit of the Justice Department, the Office of Intelligence Policy and Review (OIPR), "be invited" to all meetings between the FBI and the Criminal Division involving consultations for the purpose of coordinating efforts "to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism, or clandestine intelligence activities by foreign powers or their agents." If representatives of OIPR are unable to attend such meetings, "OIPR shall be apprized of the substance of the meetings forthwith in writing so that the Court may be notified at the earliest opportunity."

---

[123] Statistics compiled by the Electronic Privacy Information Center show that of 35,333 FISA warrants applications, only 12 were rejected between 1979 and 2013, with 532 being granted after modification. This may explain why few appeals occurred; there is no way to appeal a warrant grant, only a denial. https://epic.org/foreign-intelligence-surveillance-court-fisc/fisa-stats/

These restrictions are not original to the order appealed. They were actually set forth in an opinion written by the former Presiding Judge of the FISA court on May 17 of this year. But since that opinion did not accompany an order conditioning an approval of an electronic surveillance application it was not appealed. It is, however, the basic decision before us and it is its rationale that the government challenges. The opinion was issued after an oral argument before all of the then-serving FISA district judges and clearly represents the views of all those judges.

We think it fair to say, however, that the May 17 opinion of the FISA court does not clearly set forth the basis for its decision. It appears to proceed from the assumption that FISA constructed a barrier between counterintelligence/intelligence officials and law enforcement officers in the Executive Branch—indeed, it uses the word "wall" popularized by certain commentators (and journalists) to describe that supposed barrier.

The "wall" emerges from the court's implicit interpretation of FISA. The court apparently believes it can approve applications for electronic surveillance only if the government's objective is *not* primarily directed toward criminal prosecution of the foreign agents for their foreign intelligence activity. But the court neither refers to any FISA language supporting that view, nor does it reference the Patriot Act amendments, which the government contends specifically altered FISA to make clear that an application could be obtained even if criminal prosecution is the primary counter mechanism.

Instead the court relied for its imposition of the disputed restrictions on its statutory authority to approve "minimization procedures" designed to prevent the acquisition, retention, and dissemination within the government of material gathered in an electronic surveillance that is unnecessary to the government's need for foreign intelligence information. 50 U.S.C. § 1801(h).

The 1978 FISA

We turn first to the statute as enacted in 1978. It authorizes a judge on the FISA court to grant an application for an order approving electronic surveillance to "obtain foreign intelligence information" if "there is probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power," and that "each of the facilities or places at which the surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3). As is apparent, the definitions of agent of a foreign power and foreign intelligence information are crucial to an understanding of the statutory scheme.[8] The latter means

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> > A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> >
> > B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
> >
> > C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

The definition of an agent of a foreign power, if it pertains to a U.S. person (which is the only category relevant to this case), is closely tied to criminal activity. The term includes any person who "knowingly engages in clandestine intelligence gathering activities . . . which activities involve or may involve a violation of the *criminal statutes* of the United States," or

[8] Foreign power is defined broadly to include, *inter alia,* "a group engaged in international terrorism or activities in preparation therefor" and "a foreign-based political organization, not substantially composed of United States persons." 50 U.S.C. §§ 1801(a)(4), (5).

"knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor."

In light of these definitions, it is quite puzzling that the Justice Department, at some point during the 1980s, began to read the statute as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents—even for foreign intelligence crimes. To be sure, section 1804, which sets forth the elements of an application for an order, required a national security official in the Executive Branch—typically the Director of the FBI—to certify that "the purpose" of the surveillance is to obtain foreign intelligence information (amended by the Patriot Act to read "a significant purpose"). But as the government now argues, the definition of foreign intelligence information includes evidence of crimes such as espionage, sabotage or terrorism. Indeed, it is virtually impossible to read the 1978 FISA to exclude from its purpose the prosecution of foreign intelligence crimes, most importantly because, as we have noted, the definition of an agent of a foreign power—if he or she is a U.S. person—is grounded on criminal conduct.

It does not seem that FISA, at least as originally enacted, even contemplated that the FISA court would inquire into the government's purpose in seeking foreign intelligence information. Section 1805, governing the standards a FISA court judge is to use in determining whether to grant a surveillance order, requires the judge to find that

> the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

50 U.S.C. § 1805(a)(5). And section 1804(a)(7)(E) requires that the application include "a statement of the basis of the certification that—(i) the information sought is the type of foreign intelligence information designated; and (ii) such information cannot reasonably be obtained by normal investigative techniques." That language certainly suggests that, aside from the probable cause, identification of facilities, and minimization procedures the judge is to determine and approve, the only other issues are whether electronic surveillance is necessary to obtain the information and whether the information sought is actually foreign intelligence information—not the government's proposed use of that information.

The government argues persuasively that arresting and prosecuting terrorist agents of, or spies for, a foreign power may well be the best technique to prevent them from successfully continuing their terrorist or espionage activity. The government might wish to surveil the agent for some period of time to discover other participants in a conspiracy or to uncover a foreign power's plans, but typically at some point the government would wish to apprehend the agent and it might be that only a prosecution would provide sufficient incentives for the agent to cooperate with the government. Indeed, the threat of prosecution might be sufficient to "turn the agent."

The Patriot Act and the FISA Court's Decision

The passage of the Patriot Act altered and to some degree muddied the landscape. In October 2001, Congress amended FISA to change "the purpose" language in 1804(a)(7)(B) to "a significant purpose." It also added a provision allowing "Federal officers who conduct electronic surveillance to acquire foreign intelligence information" to "consult with Federal law enforcement officers to coordinate efforts to investigate or protect against" attack or other grave hostile acts, sabotage or international terrorism, or clandestine intelligence activities, by foreign powers or their agents. And such coordination "shall not preclude" the government's certification that a significant purpose of the surveillance is to obtain foreign intelligence information, or the issuance of an order authorizing the surveillance. Although the Patriot Act amendments to FISA expressly sanctioned consultation and coordination between intelligence

and law enforcement officials, in response to the first applications filed by OIPR under those amendments, in November 2001, the FISA court for the first time adopted the 1995 Procedures, as augmented by the January 2000 and August 2001 Procedures, as "minimization procedures" to apply in all cases before the court.

The Attorney General interpreted the Patriot Act quite differently. On March 6, 2002, the Attorney General approved new "Intelligence Sharing Procedures" to implement the Act's amendments to FISA. The 2002 Procedures supersede prior procedures and were designed to permit the complete exchange of information and advice between intelligence and law enforcement officials. They eliminated the "direction and control" test and allowed the exchange of advice between the FBI, OIPR, and the Criminal Division regarding "the initiation, operation, continuation, or expansion of FISA searches or surveillance." On March 7, 2002, the government filed a motion with the FISA court, noting that the Department of Justice had adopted the 2002 Procedures and proposing to follow those procedures in all matters before the court. The government also asked the FISA court to vacate its orders adopting the prior procedures as minimization procedures in all cases and imposing special "wall" procedures in certain cases.

Unpersuaded by the Attorney General's interpretation of the Patriot Act, the court ordered that the 2002 Procedures be adopted, *with modifications,* as minimization procedures to apply in all cases. The court emphasized that the definition of minimization procedures had not been amended by the Patriot Act, and reasoned that the 2002 Procedures "cannot be used by the government to amend the Act in ways Congress has not." The court explained:

> Given our experience in FISA surveillances and searches, we find that these provisions in sections II.B and III [of the 2002 Procedures], particularly those which authorize criminal prosecutors to advise FBI intelligence officials on the initiation, operation, continuation or expansion of FISA's intrusive seizures, are designed to enhance the acquisition, retention and dissemination of *evidence for law enforcement purposes, instead* of being consistent with the need of the United States to "obtain, produce, and disseminate *foreign intelligence information*" . . . as mandated in § 1801(h) and § 1821(4).

The statute defines minimization procedures in pertinent part as:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
>
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance.

Section 1801(h) also contains the following proviso:

> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes . . . .

As is evident from the face of section 1801(h), minimization procedures are designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information which is not foreign intelligence information. The minimization procedures allow,

however, the retention and dissemination of non-foreign intelligence information which is evidence of *ordinary crimes* for preventative or prosecutorial purposes.

The FISA court's decision and order not only misinterpreted and misapplied minimization procedures it was entitled to impose, but as the government argues persuasively, the FISA court may well have exceeded the constitutional bounds that restrict an Article III court.

Accordingly, the Patriot Act amendments clearly disapprove the primary purpose test. And as a matter of straightforward logic, if a FISA application can be granted even if "foreign intelligence" is only a significant—not a primary—purpose, another purpose can be primary. One other legitimate purpose that could exist is to prosecute a target for a foreign intelligence crime. We therefore believe the Patriot Act amply supports the government's alternative argument but, paradoxically, the Patriot Act would seem to conflict with the government's first argument because by using the term "significant purpose," the Act now implies that another purpose is to be distinguished from a foreign intelligence purpose.

That leaves us with something of an analytic conundrum. On the one hand, Congress did not amend the definition of foreign intelligence information which, we have explained, includes evidence of foreign intelligence crimes. On the other hand, Congress accepted the dichotomy between foreign intelligence and law enforcement by adopting the significant purpose test. Nevertheless, it is our task to do our best to read the statute to honor congressional intent. The better reading, it seems to us, excludes from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution. We therefore reject the government's argument to the contrary. Yet this may not make much practical difference. Because, as the government points out, when it commences an electronic surveillance of a foreign agent, typically it will not have decided whether to prosecute the agent (whatever may be the subjective intent of the investigators or lawyers who initiate an investigation). So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test.

The important point is—and here we agree with the government—the Patriot Act amendment, by using the word "significant," eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses. If the certification of the application's purpose articulates a broader objective than criminal prosecution—such as stopping an ongoing conspiracy—and includes other potential non-prosecutorial responses, the government meets the statutory test. Of course, if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct—even foreign intelligence crimes—to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied.

It can be argued, however, that by providing that an application is to be granted if the government has only a "significant purpose" of gaining foreign intelligence information, the Patriot Act allows the government to have a primary objective of prosecuting an agent for a non-foreign intelligence crime. Yet we think that would be an anomalous reading of the amendment. For we see not the slightest indication that Congress meant to give that power to the Executive Branch. Accordingly, the manifestation of such a purpose, it seems to us, would continue to disqualify an application. That is not to deny that ordinary crimes might be inextricably intertwined with foreign intelligence crimes. For example, if a group of international terrorists were to engage in bank robberies in order to finance the manufacture of a bomb, evidence of the bank robbery should be treated just as evidence of the terrorist act itself. But the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.

Having determined that FISA, as amended, does not oblige the government to demonstrate to the FISA court that its primary purpose in conducting electronic surveillance is

not criminal prosecution, we are obliged to consider whether the statute as amended is consistent with the Fourth Amendment.

It is important to note that while many of FISA's requirements for a surveillance order differ from those in Title III, few of those differences have any constitutional relevance. In the context of ordinary crime, beyond requiring searches and seizures to be reasonable, the Supreme Court has interpreted the warrant clause of the Fourth Amendment to require three elements:

> First, warrants must be issued by neutral, disinterested magistrates. Second, those seeking the warrant must demonstrate to the magistrate their probable cause to believe that "the evidence sought will aid in a particular apprehension or conviction" for a particular offense. Finally, "warrants must particularly describe the 'things to be seized,'" as well as the place to be searched.

With limited exceptions not at issue here, both Title III and FISA require prior judicial scrutiny of an application for an order authorizing electronic surveillance. And there is no dispute that a FISA judge satisfies the Fourth Amendment's requirement of a "neutral and detached magistrate."

The statutes differ to some extent in their probable cause showings. Title III allows a court to enter an *ex parte* order authorizing electronic surveillance if it determines on the basis of the facts submitted in the government's application that "there is probable cause for belief that an individual is committing, has committed, or is about to commit" a specified predicate offense. FISA by contrast requires a showing of probable cause that the target is a foreign power or an agent of a foreign power. We have noted, however, that where a U.S. person is involved, an "agent of a foreign power" is defined in terms of criminal activity. Congress clearly intended a lesser showing of probable cause for these activities than that applicable to ordinary criminal cases. And with good reason—these activities present the type of threats contemplated by the Supreme Court in *Keith* when it recognized that the focus of security surveillance "may be less precise than that directed against more conventional types of crime" even in the area of *domestic* threats to national security. Congress was aware of *Keith*'s reasoning, and recognized that it applies *a fortiori* to foreign threats.

Turning then to the first of the particularity requirements, while Title III requires probable cause to believe that particular communications concerning the specified crime will be obtained through the interception, FISA instead requires an official to designate the type of foreign intelligence information being sought, and to certify that the information sought is foreign intelligence information.

With respect to the second element of particularity, although Title III generally requires probable cause to believe that the facilities subject to surveillance are being used or are about to be used in connection with the commission of a crime or are leased to, listed in the name of, or used by the individual committing the crime, FISA requires probable cause to believe that each of the facilities or places at which the surveillance is directed is being used, or is about to be used, by a foreign power or agent.

Based on the foregoing, it should be evident that while Title III contains some protections that are not in FISA, in many significant respects the two statutes are equivalent, and in some, FISA contains additional protections. Still, to the extent the two statutes diverge in constitutionally relevant areas—in particular, in their probable cause and particularity showings—a FISA order may not be a "warrant" contemplated by the Fourth Amendment. The government itself does not actually claim that it is, instead noting only that there is authority for the proposition that a FISA order is a warrant in the constitutional sense. We do not decide the issue but note that to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment.

Ultimately, the question becomes whether FISA, as amended by the Patriot Act, is a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens. *Cf. Keith* (in domestic security context, holding that standards different from those in Title III "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the government for intelligence information and the protected rights of our citizens"). To answer that question—whether the Patriot Act's disavowal of the primary purpose test is constitutional—besides comparing the FISA procedures with Title III, it is necessary to consider carefully the underlying rationale of the primary purpose test.

The main purpose of ordinary criminal law is twofold: to punish the wrongdoer and to deter other persons in society from embarking on the same course. The government's concern with respect to foreign intelligence crimes, on the other hand, is overwhelmingly to stop or frustrate the immediate criminal activity. As we discussed in the first section of this opinion, the criminal process is often used as part of an integrated effort to counter the malign efforts of a foreign power. Punishment of the terrorist or espionage agent is really a secondary objective; indeed, punishment of a terrorist is often a moot point.

The distinction between ordinary criminal prosecutions and extraordinary situations underlies the Supreme Court's approval of entirely warrantless and even suspicionless searches that are designed to serve the government's "special needs, beyond the normal need for law enforcement."

FISA's general programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers, has from its outset been distinguishable from "ordinary crime control." After the events of September 11, 2001, though, it is hard to imagine greater emergencies facing Americans than those experienced on that date.

We acknowledge, however, that the constitutional question presented by this case — whether Congress's disapproval of the primary purpose test is consistent with the Fourth Amendment— has no definitive jurisprudential answer. The Supreme Court's special needs cases involve random stops (seizures), not electronic searches. In one sense, they can be thought of as a greater encroachment into personal privacy because they are not based on any particular suspicion. On the other hand, wiretapping is a good deal more intrusive than an automobile stop accompanied by questioning.

Although the Court in *City of Indianapolis* (2000) cautioned that the threat to society is not dispositive in determining whether a search or seizure is reasonable, it certainly remains a crucial factor. Our case may well involve the most serious threat our country faces. Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from *Keith*, that FISA as amended is constitutional because the surveillances it authorizes are reasonable.

Notes

1. Were this book written in the 1990s, much would be said about the "wall" that allegedly separated counterintelligence FBI agents from criminal law enforcement agents. The basic model allowed agents on the counterintelligence side to share information with the criminal side, but was deeply skeptical of any effort to allow agents on the criminal side to direct the counterintelligence operation. There was a great deal of confusion over the rules for this separation, as discussed in the 9/11 Commission Report. After the 9/11 attacks, much changed in the counterintelligence world. The most obvious change to FISA was this shift from "primary purpose" to "significant purpose."

2. *In re Sealed Case* also mentioned minimization procedures. When a FISA warrant is submitted, it must include a description of the procedures used to limit the acquisition and retention of information concerning U.S. persons consistent with the need to obtain and retain foreign intelligence information. Further, information concerning U.S. persons shall not be disseminated in an identifiable manner without the person's consent unless the person's identity is needed to understand the foreign intelligence information or assess its importance. This is the basis of the practice of "masking." When foreign intelligence information is presented outside the immediate intelligence community, for instance to members of Congress, the identities of U.S. persons are often concealed or "masked." They are instead labeled something like "U.S. Person 1." This masking is frequently removed or not utilized when the person's identity is relevant.

FISA warrants can be sought to authorize either electronic surveillance or physical searches of persons within the United States. The FISA probable cause inquiry differs from the familiar standard applicable to traditional criminal search warrants. The statute concerns not the target's commission of a crime, but instead a target's status as "a foreign power or an agent of a foreign power."

Both foreign power and agent of a foreign power are defined terms.

Per 50 U.S.C. § 1801 (a), "foreign power" means—

1. a foreign government or any component thereof, whether or not recognized by the United States;
2. a faction of a foreign nation or nations, not substantially composed of United States persons;
3. an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
4. a group engaged in international terrorism or activities in preparation therefor;
5. a foreign-based political organization, not substantially composed of United States persons;
6. an entity that is directed and controlled by a foreign government or governments; or
7. an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

Note the breadth of this definition. Foreign powers need not be hostile to the United States or official governmental groups. A group engaged in international terrorism is a foreign power. The Order of the Garter, an English order of chivalry, is a foreign power. A foreign public university is a component of a foreign government, making it a foreign power.[124]

Per 50 U.S.C. § 1801 (b), "agent of a foreign power" means—

1. any person other than a United States person, who—
   A. acts in the United States as an officer or employee of a foreign power . . . ;
   B. acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of

[124] This seems absurd, but it follows directly from the definition. Recall that American public university employees are treated as government actors for First and Fourth Amendment purposes.

the United States, when the circumstances indicate that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

C. Omitted

D. engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

E. engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets . . . , or knowingly conspires . . . ; or

2. any person who—

A. knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

B. pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

C. knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

D. knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

E. knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

The standard for declaring a U.S. person—a citizen or lawful permanent resident— an agent of a foreign power is somewhat different and higher than the standard for declaring a non-U.S. person a foreign power. Additionally, if the target is a U.S. person, the federal officer must swear that a "violation of the criminal statutes of the United States . . . has occurred or is about to occur." 50 U.S.C. § 1804(a)(3)(A). A U.S. citizen cannot be designated an agent of a foreign power "solely upon the basis of activities protected" under the First Amendment. 50 U.S.C. § 1805(a)(2).

Many of the statements in the warrant application must be certified by "Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation." 50 U.S.C. § 1804(a)(6). These include certification that the information sought is foreign intelligence, the significant purpose of the application is to obtain foreign intelligence, and that the information cannot reasonably be obtained through normal investigative techniques, among others. 50 U.S.C. § 1804(a)(6)(A)–(G). Due to the need for high-level approval, internal agency processes for reviewing FISA applications are fairly stringent. Defenders of the FISA process point to these internal controls

as a justification for the exceedingly high grant rate for FISA warrants—bad warrants, in their view, are almost never submitted for judicial evaluation.

The judge reviews the application through an *ex parte* proceeding, which may be supplemented by designated *amici curiae*. Most importantly, the judge must determine whether there is probable cause to believe that the target is a foreign power or agent of a foreign power and that the facilities subject to electronic surveillance are being used or about to be used by a foreign power or agent of a foreign power. The Court determines probable cause based on the target's past actions and "the facts and circumstances relating to current or future activities of the target." 50 U.S.C. § 1805(b)

This would be a natural place to insert a case that determined whether a person was an agent of a foreign power. Such cases, however, are either full of redactions to protect classified information or simply omit any useful discussion. Consider the entirety of the probable cause discussion in *United States v. Aziz*, 228 F.Supp.3d 363 (M.D. Penn. 2017).

> The defendant does not dispute that ISIL is a group engaged in international terrorism or activities in preparation therefor, thus qualifying as a foreign power under § 1804(a)(4). Aziz instead disputes the United States' ability to show that he is an agent acting for or on behalf of that foreign power. He suggests, based on evidence disclosed thus far, that the FISA applications were impermissibly based on protected First Amendment activities. Aziz also refers to controversial intelligence-gathering techniques—to wit: the warrantless Terrorist Surveillance Program and surveillance conducted pursuant to either § 1881a of the FAA or Executive Order 12,333—in questioning the reliability of the information submitted to the FISC.
>
> The court has retraced the FISC record bearing each of Aziz's concerns in mind. We have no difficulty concluding that the government satisfied all statutory requisites in this case. In each application, the government established probable cause to believe that the target of the surveillance and searches was an agent of a foreign power, and that the facilities, premises, or places to be searched were being used or were about to be used by the agent of a foreign power. In this regard, the government's filings were quite detailed, describing at length the many facts supporting its certification that a "significant purpose" of the surveillance and searches was to obtain foreign intelligence information.
>
> We also find that the applications were grounded in conduct which plainly exceeds the bounds of the First Amendment's protective sphere. Hence, the FISC orders in this case do no violence to the target's First Amendment rights. The record is devoid of any evidence that the government's intelligence-gathering efforts in this case fell within any category deemed questionable by defense counsel. The court finds ample probable cause to support the FISC orders.

One challenge throughout this entire area of law is that there are few public adversarial proceedings. FISA warrants applications are *ex parte* and most FISA surveillance does not generate subsequent criminal proceedings, meaning that almost no information about the surveillance enters the public domain. When FISA evidence is used in criminal proceedings, defense counsel has limited access to the material that was used to support the initial warrant application. And, even when the defense does try to challenge the validity of a FISA warrant, the resultant decision is usually not informative.

United States v. Aziz, 228 F.Supp.3d 363 (M.D. Penn. 2017)

Christopher C. Conner, Chief Judge

Congress enacted FISA in response to perceived abuses of intelligence-gathering and surveillance procedures by federal intelligence agencies in the early 1970s. The act establishes a statutory framework under which executive branch agencies may conduct surveillance and searches in foreign intelligence investigations.

FISA's application requirements are rigorous by design. The statute obliges the government to make detailed factual showings about the target of the proposed surveillance or search, the information sought, and the facilities at which the surveillance or search are directed. The application must be personally reviewed and approved by the Attorney General of the United States before submission to the FISC.

FISA authorizes the government to use information obtained or derived from FISC–authorized electronic surveillance or physical searches in federal, state, or local criminal prosecutions. The government must provide notice to the court and to each "aggrieved person" of its intent to disclose or to use such information. The "aggrieved person" may then move to suppress FISA-acquired evidence on grounds that "the information was unlawfully acquired" or the surveillance or search "was not made in conformity with an order of authorization or approval."

Aziz filed the instant motion to suppress and for disclosure of FISA-related information pursuant to 50 U.S.C. §§ 1806(e) and 1825(f). Aziz moors his requests in a combination of procedural, statutory, and constitutional challenges to FISA generally and as applied in this case.

FISA's statutory language is unequivocal that disclosure of warrant applications and supporting materials is the exception, not the rule. When, in answer to a suppression motion, the Attorney General files an affidavit stating "under oath that disclosure or an adversary hearing would harm the national security," the district court "shall . . . review *in camera* and *ex parte* the application, order, and such other materials relating to" the surveillance or search to determine whether intelligence-gathering was "lawfully authorized and conducted." The court may disclose "portions of" the underlying applications and supporting materials to the aggrieved person "only where such disclosure is necessary to make an accurate determination of the legality" of the surveillance or search. Courts interpreting this language have uniformly held that *in camera* and *ex parte* hearings are the "rule" and that disclosure is the "exception, occurring *only* when necessary."

The government correctly observes that every court but one to have addressed a similar motion has found disclosure to be unnecessary. The only district court to order disclosure was overturned swiftly on appeal. But to the extent the government intimates that disclosure is inappropriate merely because it is unprecedented, we reject the suggestion. That disclosure has not previously been ordered does not foreclose the possibility.

Moreover, the court questions whether this consensus accurately reflects Congressional intent. The statute is explicit in acknowledging that there may arise circumstances when "disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. §§ 1806(f), 1825(g). The legislative history reveals that Congress may not have intended to place the disclosure option so far out of reach:

> Thus, in *some* cases, the Court will likely be able to determine the legality of the surveillance without any disclosure to the defendant. In other cases, however, the question may be more complex because of, for example, indications of possible misrepresentation of fact, vague identification of the persons to be surveilled or surveillance records which include[ ] a significant amount of nonforeign

> intelligence information . . . . In such cases, the committee contemplates that the court will likely decide to order disclosure to the defendant, in whole or in part, since such disclosure "is necessary to make an accurate determination of the legality of the surveillance."

We review Aziz's disclosure request scrupulously, adhering to constitutional principles and statutory dictates.

Attorney General Loretta E. Lynch executed a declaration and claim of privilege asserting that disclosure of the FISA materials would harm national security. The Attorney General's declaration is supported by classified declaration of Carl Ghattas, Assistant Director of the Counterterrorism Division of the Federal Bureau of Investigation. The declarations and assertion of privilege are subject to "minimal scrutiny," and we may not "second-guess" the Attorney General's representations. In light of this claim of privilege, FISA permits disclosure only if an *in camera* and *ex parte* review of the materials reveals that disclosure is necessary for an accurate determination of the legality of the surveillance or search.

Aziz maintains that the government's failure to disclose FISA materials transgresses the Fourth, Fifth, and Sixth Amendments and eviscerates the very purpose of our adversary system of justice. Aziz alleges that FISA allows the government to reverse engineer prosecutions, concealing their "most intrusive and controversial surveillance methods . . . in order to thwart any adversarial challenge." Aziz exhorts that these considerations, both separately and together, jeopardize his right to a fair trial.

Congress was neither unmindful to these concerns nor unaware of its deviation from traditional adversarial practice. In enacting FISA, Congress sought to achieve parity among two critical but competing interests—to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." S. Rep. No. 95–701. The net effect is that a defendant's rights remain protected, not through traditional notice or disclosure channels, but through the "in-depth oversight of FISA surveillance by all three branches of government . . . ." This system of legislative, executive, and judicial supervision adequately guards a defendant's constitutional rights. Indeed, FISA's *ex parte* review provisions have withstood every Fourth, Fifth, and Sixth Amendment challenge levied against them. We find no constitutional deficiency in FISA's notice and disclosure provisions.

In providing for *in camera* and *ex parte* review, Congress entrusted district courts to meticulously review the FISA record for any indication of unlawfulness and to authorize disclosure when "necessary" to protect the defendant's rights. 50 U.S.C. §§ 1806(f), 1825(g). This court has complied with the statutory directive. We can fairly characterize the FISA materials in the instant case as "uncomplicated." Our inspection reveals no evidence or indication of irregularity, inconsistency, or insufficiency which might warrant disclosure to defense counsel of any portion of the FISA materials.

For the same reason, Aziz's invocation of the Federal Rules of Criminal Procedure also falls flat. Aziz suggests that Rules 12 and 16 at minimum demand notice of the methods of surveillance or searches conducted. Congress intentionally replaced these discovery rules with FISA's disclosure framework. In other words, Congress "rendered Rule 16 and other existing laws inapplicable to discovery" in the FISA context.

Aziz also requests that the court convene a *Franks* hearing to allow counsel to test the veracity of the FISA applications. A criminal defendant may challenge the truthfulness of factual statements in an affidavit of probable cause through what is commonly referred to as a *Franks* proceeding. *See Franks v. Delaware* (1978). When a defendant makes "a substantial preliminary showing" that the affidavit in question contains a false statement which was both knowingly or recklessly made and material to the finding of probable cause, the court must conduct an evidentiary hearing to examine the sufficiency of the affidavit. At minimum, the

defendant's preliminary showing must include an "offer of proof." Sufficient proof includes "affidavits or sworn or otherwise reliable" statements.

Aziz's efforts to meet his preliminary burden are necessarily speculative. The court is not insensitive to the plight of defense counsel, who must endeavor to establish the falsity of statements that the law does not allow him to see. On the other hand, the court cannot repudiate FISA's disclosure provisions by granting full access to classified material when a defendant lodges conjectural allegations of impropriety. In the exceptional context of FISA cases, the defendant's preliminary burden for a *Franks* review is all but insurmountable. In recognition thereof, Congress mandated careful *ex parte* and *in camera* judicial review of the FISA record. In essence, the court's independent review may supplant that of defense counsel.

Notes

1. When evidence from surveillance authorized by a FISA warrant is to be used in a criminal proceeding, review of the pedigree of that evidence—the warrant authorizing it, the materials and claims supporting the warrant, much of the investigative techniques used to generate the evidence—will be sharply limited. The *Aziz* judge refers to the defendant's burden to even get a hearing as "all but insurmountable." Every court to examine this process, however, has held it to be constitutional. The actual evidence being used at trial does need to be made available to the defendant, however. The government therefore must be careful who they charge, and based on what evidence, if the mere existence of the evidence would reveal classified methods.
2. Evidence obtained during FISA surveillance can be used to prosecute crimes that are entirely unrelated to foreign intelligence, and can even be used against people who were not the targets of the surveillance. In the tragic case of *State v. Isa*, 850 S.W.2d 876 (Mo. 1993), audio of the murder of sixteen-year-old Palestina Isa, which was recorded as part of FISA-authorized surveillance, was used to prosecute both of her parents. Though the FISA warrant was aimed at her father Zein, its fruits were also used against her mother Maria. Both Maria and Zein had standing to challenge the FISA warrant as "aggrieved" individuals, but the fact that Maria was not a target of the surveillance was not a basis to exclude the evidence from her criminal trial.
3. Recall that under FISA minimization procedures information unrelated to foreign intelligence is not supposed to be retained or disclosed. This does not apply to evidence of domestic crimes. "[W]hen a monitoring agent overhears evidence of domestic criminal activity, it would be a subversion of his oath of office if he did not forward that information to the proper prosecuting authorities." *United States v. Hawamda*, No. CRIM. 89-56-A, 1989 WL 235836, at *2 (E.D. Va. 1989). Moreover, FISA specifically contemplates that information will be turned over for use in criminal proceedings. 50 U.S.C. § 1806(b).

C. National Security Letters

FISA warrants allow the government to wiretap conversations, monitor email communications, and conduct physical searches. But they are not the only tool used to gather information for national security purposes domestically. A National Security Letter (NSL) is an order similar to an administrative subpoena issued by select government officials requesting customer or consumer transaction information for national security investigations.[125] NSLs operate similarly to administrative subpoenas and are issued to financial institutions, credit agencies, and communications providers. NSLs are authorized in five statutes: the Electronic

[125] CONG, RSCH. SERV., RL33320, NATIONAL SECURITY IN FOREIGN INTELLIGENCE INVESTIGATIONS: LEGAL BACKGROUND (2015), https://crsreports.congress.gov/product/pdf/RL/RL33320.

Communications Privacy Act, Fair Credit Reporting Act, Right to Financial Privacy Act, National Security Act, and PATRIOT Act.

1) Types of National Security Letters

Electronic Communications Privacy Act (ECPA) (18 U.S.C. § 2709). The ECPA permits the FBI to issue NSLs to wire or electronic communications providers. § 2709(a). The officials authorized to certify an NSL are the FBI director or their "designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director." § 2709(b). The certification must identify the specific customer or subscriber that information is sought for and affirm that the information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." Still, the investigation cannot be based solely on "activities protected by the first amendment." § 2709(b)(1)–(2). Furthermore, if the FBI wishes to prevent the recipient from disclosing the NSL's recipient, the certifying authority must affirm that the absence of such prohibition may result in "(i) a danger to the national security of the United States; (ii) interference with a criminal, counterterrorism, or counterintelligence investigation; (iii) interference with diplomatic relations; or (iv) danger to the life or physical safety of any person." § 2709(c). This gag order provision was amended to satisfy constitutional concerns and appears verbatim in each of the national security letter statutes.

Once an NSL is issued, the information that can be accessed includes the identified customer or subscriber's name, address, length of service, and toll billing information (including call lists). § 2709(b). The FBI can only disseminate the information collected to other government agencies if it complies with the rules promulgated by the Attorney General and the "information is clearly relevant to the authorized responsibilities of such agency." § 2709(e). The statute also provides the recipient of an NSL the opportunity to seek judicial review, and the agency must notify the recipient of the availability of judicial review. § 2709(d).

Fair Credit Reporting Act (FCRA) (15 U.S.C. § 1681u). The FCRA itself contains two different processes by which information can be produced for national security purposes (the PATRIOT Act addition is described below). The first one is under § 1681u(a) and (b), which provide for issuing NSLs to consumer credit reporting agencies. An FBI official may issue an NSL if they certify in writing that such information is sought "for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities." Again, however, the investigation cannot be based solely on activities protected by the First Amendment. Only the FBI director or their "designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director" can issue the certification. Furthermore, if the FBI wishes to keep the recipient from disclosing the NSL's recipient, the certifying authority must affirm that the absence of such prohibition may result in the same dangers as under ECPA. § 1681u(d).

A NSL certified by this process can demand the identified consumer's name, address, former address, place of employment, and former place of employment, § 1681u(b), or a list of institutions at which the consumer maintains or has maintained an account, § 1681u(a).

Alternatively, a full consumer report can be demanded if the same certification is approved by a court in an *ex parte* proceeding where the court performs an *in camera* examination of the certification. § 1681u(c).

The FBI is prohibited from disseminating the collected information to other federal agencies unless it is necessary to provide or conduct a "foreign counterintelligence investigation" or if the information's target is a military member. § 1681u(g). The statute also provides the recipient of an NSL the opportunity to seek judicial review, and the agency must notify the recipient of the availability of judicial review. § 1681u(e).

PATRIOT Act Additions to FCRA (15 U.S.C. § 1681v). § 1681v is the FCRA's second statutory provision for NSLs, which reflects similar processes to § 1681u(a) and (b) except for a few key distinctions. § 1681v allows NSLs to be issued by any federal agency that is "authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism when presented." § 1681v(a). The NSL must be certified by a "supervisory official designated by the head of a Federal agency or an officer of a Federal agency" subject to a regular Constitutional appointment process—nomination by the President and confirmation by the Senate. § 1681v(b). The certifying official must affirm "that such information is necessary for the agency's conduct or such investigation, activity or analysis and that includes a term that specifically identifies a consumer or account to be used as the basis for the production of such information." § 1681v(a). Another key distinction between other FCRA NSLs is that the accessible information is broader, requiring the consumer reporting agency to give "a consumer report of a consumer and all other information in a consumer's file." § 1681v(a). The same non-disclosure, judicial review, and dissemination provisions are required outside of the abovementioned distinctions.

Right to Financial Privacy Act (RFPA) (12 U.S.C. § 3414). The RFPA authorizes the FBI to issue NSLs to financial institutions. § 3414(a). The FBI Director, "the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director" must certify in writing that the records are sought for "foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities." § 3414(a)(5)(A). The investigation cannot solely be based on activities protected by the First Amendment. The NSL may include a non-disclosure requirement if the certifying authority affirms the usual requirements.

This form of NSL can demand any of a consumer's financial records. These are defined broadly to include "any record held by a financial institution pertaining to a customer's relationship with the financial institution." § 3401(2)

Once the NSL is issued, the financial institution must provide the targeted individual's financial records in their possession. § 3414(a)(5)(A). The FBI cannot disseminate the collected information unless it complies with rules promulgated by the Attorney General and the information is "clearly relevant to the authorized responsibilities of such agency." § 3414(a)(5)(B). Additionally, judicial review exists for the recipient, and the NSL must include a notification that judicial review is available. § 3414(d).

National Security Act (50 U.S.C. § 3162). The National Security Act authorizes NSLs regarding counterintelligence operations of federal employees. An important distinction with this NSL is that it is limited to federal employees. The NSL can be directed to any "financial agency, financial institution, or holding company, or from any consumer reporting agency" or from a "commercial entity within the United States pertaining to travel." § 3162(a)(1). The NSL must be certified "by the department or agency head or deputy department or agency head concerned, or by a senior official designated for this purpose by the department or agency head concerned (whose rank shall be no lower than Assistant Secretary or Assistant Director)." § 3162(a)(3)(A). The certifying official must affirm in writing that the information sought is for an employee seeking security to access classified information and has provided consent or that there are reasonable grounds to believe that the target is an employee disclosing classified information to a "foreign power or agent of a foreign power," the circumstances indicate that the employee has "incurred excessive indebtedness" or unexplainable affluence, or the circumstances indicate that the employee can disclose classified information that has been "lost or compromised to a foreign power or agent of a foreign power." § 3162(a)(2). Each NSL must include the certification, a copy of the employee consent agreement, the specific category of records sought, and information on the availability of judicial review. § 3162(a)(3).

Once issued, the recipient must provide "such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law

enforcement investigation, counterintelligence inquiry, or security determination." § 3162(a)(1). The dissemination of collected information is limited to the agency employing the target, the Justice Department for law enforcement or counterintelligence purposes, or an agency if that the information is clearly relevant to their responsibilities. § 3162(f).

2) Constitutionality of Gag Orders

Statutes permitting NSLs all include a confidentiality clause that prevents the recipient from disclosing any information relating to the receipt of the request. Originally, these confidentiality clauses were broad, with no disclosure permitted by the recipient. *In re Three Nat'l Sec. Letters*, 35 F.4th 1181, 1185 (9th Cir. 2022). However, in 2008, the Second Circuit ruled that the statutory scheme that did not allow for judicial review and imposed broad confidentiality requirements violated the First Amendment. *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 880–81 (2d Cir. 2008), *as modified* (Mar. 26, 2009). Congress then amended the NSL statutes to clarify that judicial review was available and the recipient could disclose receipt of an NSL to their attorney or those necessary to comply.

Further revisions to the NSL disclosure statutes were implemented via the USA FREEDOM Act, requiring that the Attorney General promulgate rules to limit dissemination between agencies and to allow the recipient company to disclose the total number of NSLs. *In re Three Nat'l Sec. Letters*, 35 F.4th at 1185. The Ninth Circuit approved these measures as narrowly tailored due to their limited scope, the availability of judicial review, and the ability to report statistics on the number of letters received. *Id*. at 1058.

Notes

1. NSLs are generally aimed at metadata or envelope data rather than content data. They can get a list of who you called, but not the words you said. How easy should it be for the government to get this kind of information? Note that basic NSLs do not involve any independent judicial oversight. Consider in particular the scope of information obtainable.
2. There is an oddity when one looks at the FCRA NSLs. Protections for full consumer reports that existed prior to the PATRIOT Act are effectively removed by the PATRIOT Act; the alternative route under § 1681v is simply easier than the old one under § 1681u(c).

D. Section 215 and the metadata program

Section 215 of the PATRIOT Act gave the government the ability to apply for a new type of court order. This order could compel the production of "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." The order also carried with it a gag requirement; the recipient could not publicly disclose that they had received it. This order needed to be approved by a judge, but did not have the probable cause requirements of either FISA or the ECPA.

This provision proved deeply controversial. Upon passage, it was criticized for allowing the government to, in theory, seize library borrowing records. It was later the basis of the telephone metadata program, where the telephone dialing records of millions of Americans were seized for data mining. The government's authority under Section 215 expired in 2015, was then renewed with new restrictions on bulk collection under the USA FREEDOM Act, and then expired again in 2020.

Despite both Section 215 and its monitoring program being discontinued, it is still important to understand them. There are two reasons for this. First, no idea in surveillance ever truly goes away. The ideas behind the monitoring program will almost certainly reemerge

eventually and, for all we know, may have already been dusted off in secret. Second, the constitutional questions raised by bulk collection and analysis of data remain with us. If the government does not need a warrant to gather a type of information from one person, does it require a warrant to gather that information from 300 million people?

United States v. Moalin 973 F.3d 977 (9th Cir. 2020)

BERZON, Circuit Judge

Four members of the Somali diaspora appeal from their convictions for sending, or conspiring to send, $10,900 to Somalia to support a foreign terrorist organization. Their appeal raises complex questions regarding the U.S. government's authority to collect bulk data about its citizens' activities under the auspices of a foreign intelligence investigation, as well as the rights of criminal defendants when the prosecution uses information derived from foreign intelligence surveillance. We conclude that the government may have violated the Fourth Amendment and did violate the Foreign Intelligence Surveillance Act ("FISA") when it collected the telephony metadata of millions of Americans, including at least one of the defendants, but suppression is not warranted on the facts of this case. Additionally, we confirm that the Fourth Amendment requires notice to a criminal defendant when the prosecution intends to enter into evidence or otherwise use or disclose information obtained or derived from surveillance of that defendant conducted pursuant to the government's foreign intelligence authorities. We do not decide whether the government failed to provide any required notice in this case because the lack of such notice did not prejudice the defendants. After considering these issues and several others raised by the defendants, we affirm the convictions in all respects.

Somalia's turbulent recent history forms the backdrop for this case. After military dictator Siad Barre was ousted in 1991, the country spiraled into civil war. Fighting between rival warlords led to a humanitarian crisis in Mogadishu, Somalia's capital, and other parts of the country. An estimated 30,000 people died in Mogadishu alone, and hundreds of thousands more were displaced. As the war continued, its impact on the populace was exacerbated by recurring periods of severe drought and famine.

Many Somalis have fled the country. An estimated three million live abroad, creating a global Somali diaspora. Somalis abroad often remain actively engaged in developments in Somalia, and contributions from the diaspora are a critical source of financial support within the troubled country. As Somalia has no formal banking system, members of the diaspora who wish to send money back frequently rely on informal money transfer businesses called “hawalas.”

Defendants Basaaly Saeed Moalin, Mohamed Mohamed Mohamud, Issa Doreh, and Ahmed Nasir Taalil Mohamud immigrated to the United States from Somalia years ago and lived in Southern California.[2] Moalin and Nasir Mohamud were taxicab drivers; M. Mohamud was an imam at a mosque; and Doreh worked at Shidaal Express, a hawala.

Between October 2010 and June 2012, the United States ("the government") charged defendants in a five-count indictment with conspiring to send and sending $15,900 to Somalia between January and August of 2008 to support al-Shabaab [a designated terrorist organization].

Shortly after filing the initial indictment, the government filed notice that it intended to use or disclose in the proceedings "information obtained or derived from electronic surveillance conducted pursuant to the authority of the Foreign Intelligence Surveillance Act." At trial, the government's principal evidence against defendants consisted of a series of recorded calls between Moalin, his codefendants, and individuals in Somalia, obtained through a wiretap of

[2] Moalin and Doreh are U.S. citizens, M. Mohamud has refugee status, and Nasir Mohamud has a visa.

Moalin's phone. The government obtained access to Moalin's calls after receiving a court order under FISA. Several of the recorded calls involved a man who went by "Shikhalow" or "Majadhub," whom the government contends was Ayrow, the important al-Shabaab figure. In addition to the intercepted phone calls, the government introduced records of money transfers completed by Shidaal Express, the hawala where Doreh worked.

In a recorded call from December 2007, Shikhalow requested money from Moalin for "rations." The two men also discussed other fundraising efforts relating to a school. Moalin then spoke with Doreh, reporting that "[o]ne dollar a day per man" was needed for forces stationed "where the fighting [is] going on." Moalin also spoke with Nasir Mohamud, telling him that money was needed for "the young men who are firing the bullets" and that, within the last month, "these men cut the throats of 60" Ethiopians and destroyed up to five vehicles. In February 2013, the jury convicted defendants on all counts.

Before trial, Moalin moved to suppress, among other things, "all interceptions made and electronic surveillance conducted pursuant to [FISA] and any fruits thereof, and/or for disclosure of the underlying applications for FISA warrants." The district court denied Moalin's suppression motion and did not grant security-cleared defense counsel access to the documents supporting the FISA orders.

Months after the trial, in June 2013, former National Security Agency ("NSA") contractor Edward Snowden made public the existence of NSA data collection programs. One such program, conducted under FISA Subchapter IV, involved the bulk collection of phone records, known as telephony metadata, from telecommunications providers. Other programs, conducted under the FISA Amendments Act of 2008, involved the collection of electronic communications, such as email messages and video chats, including those of people in the United States.

Subsequent statements of public officials defending the telephony metadata collection program averred that the program had played a role in the government's investigation of Moalin. These statements reported that the FBI had previously closed an investigation focused on Moalin without bringing charges, then reopened that investigation based on information obtained from the metadata program.

For instance, in a hearing before the House Permanent Select Committee on Intelligence held shortly after the Snowden disclosures, then-FBI Deputy Director Sean Joyce described a post-9/11 investigation conducted by the FBI that initially "did not find any connection to terrorist activity. Several years later, under [FISA Subchapter IV], the NSA provided us a telephone number only in San Diego that had indirect contact with an extremist outside the United States." Joyce explained that the FBI "served legal process to identify who was the subscriber to this telephone number," then, after "further investigation and electronic surveillance that we applied specifically for this U.S. person with the FISA Court, we were able to identify co-conspirators, and we were able to disrupt" their financial support to a Somali designated terrorist group. According to Joyce, "if [the FBI] did not have the tip from NSA, [it] would not have been able to reopen that investigation." In another congressional hearing, Joyce specifically named Moalin as the target of the investigation.

On September 30, 2013, defendants filed a motion for a new trial. Defendants argued that the government's collection and use of Moalin's telephony metadata violated the Fourth Amendment, and that the government had failed to provide notice of the metadata collection or of any surveillance of Moalin it had conducted under the FISA Amendments Act, including, potentially, the surveillance referred to in the email to the linguist. The district court denied the motion, concluding that "public disclosure of the NSA program adds no new facts to alter the court's FISA . . . rulings," and that the telephony metadata program did not violate the Fourth Amendment.

I. The Telephony Metadata Collection Program

The government's telephony metadata collection program was authorized in a series of classified orders by the FISA Court under FISA Subchapter IV, the "business records" subchapter. These orders required major telecommunications providers to turn over to the government on an "ongoing daily" basis a "very large volume" of their "call detail records." Specifically, providers were ordered to produce "all call detail records or 'telephony metadata' . . . for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." These records included information such as the phone numbers involved in a call and the time and duration of the call, but not the voice content of any call.

The court orders authorized the NSA to compile the records into a database and to query the database under certain conditions to obtain foreign intelligence information. During the time period relevant to this case, the government was permitted to search the database when certain NSA officials determined that "reasonable, articulable suspicion" existed connecting a specific selection term—for example, a particular phone number—with "one of the identified international terrorist organizations." The government was also allowed to search phone numbers within three "hops" of that selector, *i.e.*, the phone numbers directly in contact with a selector, the numbers that had been in contact with those numbers, and the numbers that had been in contact with those numbers.

Snowden's disclosure of the metadata program prompted significant public debate over the appropriate scope of government surveillance. In June 2015, Congress passed the USA FREEDOM Act, which effectively ended the NSA's bulk telephony metadata collection program. The Act prohibited further bulk collection of phone records after November 28, 2015. Besides ending the bulk collection program, Congress also established new reporting requirements relating to the government's collection of call detail records.

Defendants contend that the discontinued metadata program violated both the Fourth Amendment and FISA Subchapter IV, under which it was authorized. They argue that the "fruits" of the government's acquisition of Moalin's phone records should therefore have been suppressed. According to defendants, those fruits included the phone records themselves and the evidence the government obtained through its subsequent wiretap of Moalin's phone.

Moalin asserts he had a reasonable expectation of privacy in his telephony metadata. The district court held, and the government argues, that this case is controlled by *Smith v. Maryland* (1979), which helped establish the so-called third-party doctrine in Fourth Amendment jurisprudence. *Smith* held that the government's use of a pen register to record the numbers the defendant dialed from his home telephone did not constitute a Fourth Amendment search, because individuals have no reasonable expectation of privacy in information they voluntarily convey to the telephone company. *Smith* relied on *United States v. Miller* (1976), which had held that defendants had no legitimate expectation of privacy in their bank records. The government argues that the NSA's collection of Moalin's telephony metadata is indistinguishable, for Fourth Amendment purposes, from the use of the pen register in *Smith*.

There are strong reasons to doubt that *Smith* applies here. Advances in technology since 1979 have enabled the government to collect and analyze information about its citizens on an unprecedented scale. Confronting these changes, and recognizing that a "central aim" of the Fourth Amendment was "to place obstacles in the way of a too permeating police surveillance," the Supreme Court recently declined to "extend" the third-party doctrine to information whose collection was enabled by new technology. *Carpenter v. United States* (2018).

Carpenter did not apply the third-party doctrine to the government's acquisition of historical cell phone records from the petitioner's wireless carriers. The records revealed the geographic areas in which the petitioner used his cell phone over a period of time. Citing the "unique nature of cell phone location information," the Court concluded in *Carpenter* that "the

fact that the Government obtained the information from a third party does not overcome [the petitioner's] claim to Fourth Amendment protection," because there is "a world of difference between the limited types of personal information addressed in *Smith* . . . and the exhaustive chronicle of location information casually collected by wireless carriers today."

There is a similar gulf between the facts of *Smith* and the NSA's long-term collection of telephony metadata from Moalin and millions of other Americans. In *Smith*, a woman was robbed and gave the police a description of the robber and of a car she saw nearby. After the robbery, the woman received "threatening and obscene phone calls from a man identifying himself as the robber." Police later spotted a man and car matching the robber's description and traced the license plate number to Smith. Without obtaining a warrant, they asked the telephone company to install a "pen register," a device that would record the numbers dialed from Smith's home telephone. The day the pen register was installed it recorded a call from Smith's home to the home of the robbery victim. Based on that and other evidence, police obtained a warrant to search Smith's home and arrested him two days later.

The distinctions between *Smith* and this case are legion and most probably constitutionally significant. To begin with, the type of information recorded in *Smith* was "limited" and of a less "revealing nature" than the telephony metadata at issue here. The pen register did not disclose the "identities" of the caller or of the recipient of a call, "nor whether the call was even completed." In contrast, the metadata in this case included "comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile station Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call." "IMSI and IMEI numbers are unique numbers associated with a particular telephone user or communications device." "A 'trunk identifier' provides information about where a phone connected to the network, revealing data that can locate the parties within approximately a square kilometer."

Although the *Smith* Court perceived a significant distinction between the "contents" of a conversation and the phone number dialed, in recent years the distinction between content and metadata "has become increasingly untenable," as Amici point out. The amount of metadata created and collected has increased exponentially, along with the government's ability to analyze it. "Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life." According to the NSA's former general counsel Stewart Baker, "[m]etadata absolutely tells you everything about somebody's life. . . . If you have enough metadata you don't really need content . . . ." Laura K. Donohue, *The Future of Foreign Intelligence* 39 (2016). The information collected here was thus substantially more revealing than the telephone numbers recorded in *Smith*.

The duration of the collection in this case—and so the amount of information collected—also vastly exceeds that in *Smith*. While the pen register in *Smith* was used for a few days at most, here the NSA collected Moalin's (and millions of other Americans') telephony metadata on an ongoing, daily basis for years. *Carpenter* distinguished between using a beeper to track a car "during a discrete automotive journey," which the Court had upheld in *United States v. Knotts* (1983), and using cell phone location information to reveal "an all-encompassing record of the holder's whereabouts" "over the course of 127 days." As the Court put it, "Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible."

Like the cell phone location information in *Carpenter*, telephony metadata, "as applied to individual telephone subscribers, particularly with relation to mobile phone services and when collected on an ongoing basis with respect to all of an individual's calls . . . permit something akin to . . . 24-hour surveillance . . . ." This long-term surveillance, made possible by

new technology, upends conventional expectations of privacy. Historically, "surveillance for any extended period of time was difficult and costly and therefore rarely undertaken." *United States v. Jones* (2012) (Alito, J., concurring in the judgment). Society may not have recognized as reasonable Smith's expectation of privacy in a few days' worth of dialed numbers but is much more likely to perceive as private several years' worth of telephony metadata collected on an ongoing, daily basis—as demonstrated by the public outcry following the revelation of the metadata collection program.

Also problematic is the extremely large number of people from whom the NSA collected telephony metadata, enabling the data to be aggregated and analyzed in bulk. The government asserts that "the fact that the NSA program also involved call records relating to other people . . . is irrelevant because Fourth Amendment rights . . . cannot be raised vicariously." The government quotes the FISA Court, which reasoned similarly that "where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*." [*In Re FBI*]. But these observations fail to recognize that the collection of millions of other people's telephony metadata, and the ability to aggregate and analyze it, makes the collection of Moalin's *own* metadata considerably more revealing.

A couple of examples illustrate this point: A woman calls her sister at 2:00 a.m. and talks for an hour. The record of that call reveals some of the woman's personal information, but more is revealed by access to the sister's call records, which show that the sister called the woman's husband immediately afterward. Or, a police officer calls his college roommate for the first time in years. Afterward, the roommate calls a suicide hotline. These are simple examples; in fact, metadata can be combined and analyzed to reveal far more sophisticated information than one or two individuals' phone records convey. As Amici explain, "it is relatively simple to superimpose our metadata trails onto the trails of everyone within our social group and those of everyone within our contacts' social groups and quickly paint a picture that can be startlingly detailed"—for example, "identify[ing] the strength of relationships and the structure of organizations." Thus, the very large number of people from whom telephony metadata was collected distinguishes this case meaningfully from *Smith*.

Finally, numerous commentators and two Supreme Court Justices have questioned the continuing viability of the third-party doctrine under current societal realities. The assumption-of-risk rationale underlying the doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones* (Sotomayor, J., concurring). "Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* . . . teach[es] that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did." *Carpenter* (Gorsuch, J., dissenting).

For all these reasons, defendants' Fourth Amendment argument has considerable force. But we do not come to rest as to whether the discontinued metadata program violated the Fourth Amendment because even if it did, suppression would not be warranted on the facts of this case. Having carefully reviewed the classified FISA applications and all related classified information, we are convinced that under established Fourth Amendment standards, the metadata collection, even if unconstitutional, did not taint the evidence introduced by the government at trial. To the extent the public statements of government officials created a contrary impression, that impression is inconsistent with the contents of the classified record.

Defendants also argue that the metadata collection program violated FISA Subchapter IV, under which the FISA Court authorized it. At the time relevant to this case, the statute required the government to include in its application "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are *relevant to an authorized investigation* (other than a threat assessment)." 50 U.S.C. § 1861(b)(2)(A) (2006) (emphasis

added). Defendants argue that the metadata program defied this relevance requirement because the government collected phone records in bulk, without regard to whether any individual record was relevant to any specific, already-authorized investigation.

[W]e do not accept the government's justification in this case that "the call detail records at issue *here*—the records that suggested that a particular U.S.-based telephone number may have been associated with a foreign terrorist—were clearly relevant to a counterterrorism investigation." That argument depends on an after-the-fact determination of relevance: once the government had collected a massive amount of call records, it was able to find one that was relevant to a counterterrorism investigation. The problem, of course, is that FISA required the government to make a showing of relevance to a particular authorized investigation *before* collecting the records. We hold that the telephony metadata collection program exceeded the scope of Congress's authorization in section 1861 and therefore violated that section of FISA.

As a remedy for the FISA violation, defendants ask us to suppress the alleged "fruits" of the unlawful metadata collection, including the evidence from the government's wiretap of Moalin's phone. Because "suppression is a disfavored remedy," we impose it to remedy a statutory violation "only . . . where it is clearly contemplated by the relevant statute."

To obtain the Moalin wiretap order, the government submitted an application to the FISA Court including, among other things, "a statement of the facts and circumstances relied upon by the applicant to justify his belief that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power." Contrary to defendants' assumption, the government maintains that Moalin's metadata "did not and was not necessary to support the requisite probable cause showing" for the Subchapter I application in this case. Our review of the classified record confirms this representation. Even if we were to apply a "fruit of the poisonous tree" analysis, we would conclude, based on our careful review of the classified FISA applications and related information, that the FISA wiretap evidence was not the fruit of the unlawful metadata collection. Again, if the statements of public officials created a contrary impression, that impression is inconsistent with the facts presented in the classified record. Because the wiretap evidence was not "unlawfully acquired," suppression is not warranted.

II. Notice of Surveillance Activities

Separately from their contention that the metadata collection violated their Fourth Amendment rights, defendants maintain that the Fourth Amendment required the government to provide notice to defendants of its collection and use of Moalin's telephony metadata.

The Fourth Amendment requires that a person subject to a government search receive notice of the search, absent "exigent circumstances." [T]he need for secrecy inherent in foreign intelligence investigations justifies a more circumscribed notice requirement than in the ordinary criminal context. Whereas the Wiretap Act requires notice at the end of an investigation regardless of whether an indictment is filed, the FISA and FAA notice provisions are more limited, requiring notice only when the "Government intends to enter into evidence or otherwise use or disclose in any trial . . . or other proceeding in or before any court . . . or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter."

We emphasize that notice is distinct from disclosure. Given the need for secrecy in the foreign intelligence context, the government is required only to inform the defendant that surveillance occurred and that the government intends to use information obtained or derived from it. Knowledge of surveillance will enable the defendant to file a motion with the district court challenging its legality. If the government avers that disclosure of information relating to the surveillance would harm national security, then the court can review the materials bearing on its legality *in camera* and *ex parte.*

Here, assuming without deciding that the government should have provided notice of the metadata collection to defendants, the government's failure to do so did not prejudice defendants. Defendants learned of the metadata collection, albeit in an unusual way, in time to challenge the legality of the program in their motion for a new trial and on appeal.

Notes

1.) The constitutionality of the metadata program has not been definitively ruled upon. The Ninth Circuit is not the Supreme Court, and even it was not speaking especially clearly here on the constitutionality of the metadata program. Earlier decisions from other courts were split. The simplest argument for the constitutionality of the metadata program was expressed in *In Re F.B.I. for an Order Requiring the Production of Tangible Things from [Redacted]* No. BR 13-109, 2013 WL 5741573 (FISA Ct. 2013):

> Here, the government is requesting daily production of certain telephony metadata in bulk belonging to companies without specifying the particular number of an individual. This Court had reason to analyze this distinction in a similar context in [redacted]. In that case, this Court found that "regarding the breadth of the proposed surveillance, it is noteworthy that the application of the Fourth Amendment depends on the government's intruding into some individual's reasonable expectation of privacy." The Court noted that Fourth Amendment rights are personal and individual, and that "[s]o long as no individual has a reasonable expectation of privacy in meta data, the large number of persons whose communications will be subjected to the . . . surveillance is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur." Put another way, where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*.
>
> In sum, because the Application at issue here concerns only the production of call detail records or "telephony metadata" belonging to a telephone company, and not the contents of communications, *Smith v. Maryland* compels the conclusion that there is no Fourth Amendment impediment to the collection. Furthermore, for the reasons stated in and discussed above, this Court finds that the volume of records being acquired does not alter this conclusion. Indeed, there is no legal basis for this Court to find otherwise.[126]

2.) The tension between *Moalin* and *In Re F.B.I.* underlies many major questions of Fourth Amendment law. A person does not have an expectation of privacy on public roads. Does that mean that the government can surveil everyone on public roads at all times? If it does not mean that, how does one explain the distinction?

3.) Following the 2013 Edward Snowden leaks, which revealed the metadata collection program, there was considerable debate over the program's desirability. In 2015, the USA Freedom Act was passed to reform the program. The primary contribution of the act was to prevent the bulk collection of telephone metadata. Instead, telephone companies would provide records to the government on a targeted case-by-case basis. Previously the metadata requests had not included a specific selection term—the complete dataset of millions of call records was sent to the government and only there were targeted searches run. Under the amended program, the government would send specific identifiers (such as telephone numbers or device IDs) to the companies and the companies would then run the analyses and send relevant hits back to the government. Further, applications needed to show

[126] This is a declassified opinion from the Foreign Intelligence Surveillance Court. It is available at https://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf

reasonable articulable suspicion that the specific selection term used was associated with a foreign power or agent of a foreign power engaged in terrorism. Implementation of these changes proved very technically difficult. In 2020, the authorization provided by the USA Freedom Act expired and, largely due to President Trump's opposition, it was not renewed.

4.) Did the metadata collection program ever work? Quite possibly not. A retrospective review of the program looking at results from 2015 through 2019 concluded that the program cost 100 million dollars and only resulted in two unique leads, only one of which led to a significant intelligence investigation.[127] The program prior to 2015 also did not claim large successes. A 2014 report by the U.S. Privacy and Civil Liberties Oversight Board stated:

> Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect [namely Basaaly Moalin].[128]

E. Section 702 and surveillance overseas

Today, FISA has two main tracks for surveillance. The usual warrant process is used for the surveillance of both non-US persons who are physically in the United States and as well as US persons. Section 702 of the FISA Amendments Act of 2008, however, allows for surveillance of foreign persons located overseas whose communications are transmitted through US facilities.

Section 702 grew out of concerns raised by President Bush's Terrorist Surveillance Program. This initiative, created in the wake of the 9/11 attacks, collected emails and wiretapped phones as long as one party was not a U.S. person. When this program was revealed to the public however, it was substantially criticized for its incidental interception of American communications.

In response to these concerns, Congress passed the FISA Amendments Act of 2008 ("FAA"), which created Section 702. Section 702 permits warrantless electronic surveillance of foreign targets whom the federal government reasonably believes to be overseas, even if those targets may be communicating with people in the United States. Importantly, Section 702 prohibits warrantless surveillance if the purpose is to target a particular person known or reasonably believed to be in the United States. FISC preapproves the procedures for conducting warrantless searches and minimizes the risk of surveilling U.S. Citizens. Under 702, federal officials can force telecommunications service providers to provide emails or other electronic communications.

---

[127] Charlie Savage, *N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads*, N.Y. TIMES (Feb. 25, 2020), https://www.nytimes.com/2020/02/25/us/politics/nsa-phone-program.html.

[128] PRIV. AND CIV. LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/cf0ce183-7935-4b06-bb41-007d1f437412/215-Report_on_the_Telephone_Records_Program%20-%20Completed%20508%20-%2011292022.pdf.

The role of 702 is especially large given the power of US technology companies. Many people overseas use services provided by companies that are headquartered in the United States and subject to American legal process.

The constitutionality of 702 has been challenged in a variety of cases. One of the earliest and most famous cases failed before the Supreme Court on procedural grounds, specifically a lack of federal Article III standing.

Clapper v. Amnesty Intern. USA, 568 U.S. 398 (2013)

Justice ALITO delivered the opinion of the Court.

Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a, allows the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not "United States persons" and are reasonably believed to be located outside the United States. Before doing so, the Attorney General and the Director of National Intelligence normally must obtain the Foreign Intelligence Surveillance Court's approval. Respondents are United States persons whose work, they allege, requires them to engage in sensitive international communications with individuals who they believe are likely targets of surveillance under § 1881a. Respondents seek a declaration that § 1881a is unconstitutional, as well as an injunction against § 1881a-authorized surveillance.

Respondents assert that they can establish injury in fact because there is an objectively reasonable likelihood that their communications will be acquired under § 1881a at some point in the future. But respondents' theory of *future* injury is too speculative to satisfy the well-established requirement that threatened injury must be "certainly impending." And even if respondents could demonstrate that the threatened injury is certainly impending, they still would not be able to establish that this injury is fairly traceable to § 1881a. As an alternative argument, respondents contend that they are suffering *present* injury because the risk of § 1881a-authorized surveillance already has forced them to take costly and burdensome measures to protect the confidentiality of their international communications. But respondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending. We therefore hold that respondents lack Article III standing.

In 1978, after years of debate, Congress enacted the Foreign Intelligence Surveillance Act (FISA) to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes. In enacting FISA, Congress legislated against the backdrop of our decision in *United States v. United States Dist. Court for Eastern Dist. of Mich.* (1972) (*Keith*), in which we explained that the standards and procedures that law enforcement officials must follow when conducting "surveillance of 'ordinary crime' " might not be required in the context of surveillance conducted for domestic national-security purposes. Although the *Keith* opinion expressly disclaimed any ruling "on the scope of the President's surveillance power with respect to the activities of foreign powers," it implicitly suggested that a special framework for foreign intelligence surveillance might be constitutionally permissible.

When Congress enacted the FISA Amendments Act of 2008 (FISA Amendments Act), it left much of FISA intact, but it "established a new and independent source of intelligence collection authority, beyond that granted in traditional FISA." As relevant here, § 702 of FISA, 50 U.S.C. § 1881a, supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting the communications of non-U.S. persons located abroad. Unlike traditional FISA surveillance, § 1881a does not require the Government to demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power. And, unlike traditional FISA, § 1881a does not require the Government to specify

the nature and location of each of the particular facilities or places at which the electronic surveillance will occur.

The present case involves a constitutional challenge to § 1881a. Section 1881a mandates that the Government obtain the Foreign Intelligence Surveillance Court's approval of "targeting" procedures, "minimization" procedures, and a governmental certification regarding proposed surveillance. Among other things, the Government's certification must attest that (1) procedures are in place "that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the [FISC] that are reasonably designed" to ensure that an acquisition is "limited to targeting persons reasonably believed to be located outside" the United States; (2) minimization procedures adequately restrict the acquisition, retention, and dissemination of nonpublic information about unconsenting U.S. persons, as appropriate; (3) guidelines have been adopted to ensure compliance with targeting limits and the Fourth Amendment; and (4) the procedures and guidelines referred to above comport with the Fourth Amendment.

The Foreign Intelligence Surveillance Court's role includes determining whether the Government's certification contains the required elements. Additionally, the Court assesses whether the targeting procedures are "reasonably designed" (1) to "ensure that an acquisition ... is limited to targeting persons reasonably believed to be located outside the United States" and (2) to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known ... to be located in the United States." The Court analyzes whether the minimization procedures "meet the definition of minimization procedures under section 1801(h) ..., as appropriate." The Court also assesses whether the targeting and minimization procedures are consistent with the statute and the Fourth Amendment.

Respondents are attorneys and human rights, labor, legal, and media organizations whose work allegedly requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad. Respondents believe that some of the people with whom they exchange foreign intelligence information are likely targets of surveillance under § 1881a. Specifically, respondents claim that they communicate by telephone and e-mail with people the Government "believes or believed to be associated with terrorist organizations," "people located in geographic areas that are a special focus" of the Government's counterterrorism or diplomatic efforts, and activists who oppose governments that are supported by the United States Government. App. to Pet. for Cert. 399a.

Respondents claim that § 1881a compromises their ability to locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients. Respondents also assert that they "have ceased engaging" in certain telephone and e-mail conversations. According to respondents, the threat of surveillance will compel them to travel abroad in order to have in-person conversations. In addition, respondents declare that they have undertaken "costly and burdensome measures" to protect the confidentiality of sensitive communications.

Article III of the Constitution limits federal courts' jurisdiction to certain "Cases" and "Controversies." As we have explained, "[n]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." "One element of the case-or-controversy requirement" is that plaintiffs "must establish that they have standing to sue."

The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches. In keeping with the purpose of this doctrine, "[o]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." "Relaxation of

standing requirements is directly related to the expansion of judicial power," and we have often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs.

To establish Article III standing, an injury must be "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending." Thus, we have repeatedly reiterated that "threatened injury must be *certainly impending* to constitute injury in fact," and that "[a]llegations of *possible* future injury" are not sufficient.

Respondents assert that they can establish injury in fact that is fairly traceable to § 1881a because there is an objectively reasonable likelihood that their communications with their foreign contacts will be intercepted under § 1881a at some point in the future. This argument fails. As an initial matter, the Second Circuit's "objectively reasonable likelihood" standard is inconsistent with our requirement that "threatened injury must be certainly impending to constitute injury in fact." Furthermore, respondents' argument rests on their highly speculative fear that: (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts. As discussed below, respondents' theory of standing, which relies on a highly attenuated chain of possibilities, does not satisfy the requirement that threatened injury must be certainly impending. Moreover, even if respondents could demonstrate injury in fact, the second link in the above-described chain of contingencies—which amounts to mere speculation about whether surveillance would be under § 1881a or some other authority—shows that respondents cannot satisfy the requirement that any injury in fact must be fairly traceable to § 1881a.

First, it is speculative whether the Government will imminently target communications to which respondents are parties. Section 1881a expressly provides that respondents, who are U.S. persons, cannot be targeted for surveillance under § 1881a. Accordingly, it is no surprise that respondents fail to offer any evidence that their communications have been monitored under § 1881a, a failure that substantially undermines their standing theory. Indeed, respondents do not even allege that the Government has sought the FISC's approval for surveillance of their communications. Accordingly, respondents' theory necessarily rests on their assertion that the Government will target *other individuals*—namely, their foreign contacts.

Yet respondents have no actual knowledge of the Government's § 1881a targeting practices. Instead, respondents merely speculate and make assumptions about whether their communications with their foreign contacts will be acquired under § 1881a. For example, journalist Christopher Hedges states: "I have no choice but to *assume* that any of my international communications *may* be subject to government surveillance, and I have to make decisions ... in light of that *assumption*." "The party invoking federal jurisdiction bears the burden of establishing" standing—and, at the summary judgment stage, such a party "can no longer rest on ... 'mere allegations,' but must 'set forth' by affidavit or other evidence 'specific facts.' " *Defenders of Wildlife*. Respondents, however, have set forth no specific facts demonstrating that the communications of their foreign contacts will be targeted. Moreover, because § 1881a at most *authorizes*—but does not *mandate* or *direct*—the surveillance that respondents fear, respondents' allegations are necessarily conjectural. Simply put, respondents

can only speculate as to how the Attorney General and the Director of National Intelligence will exercise their discretion in determining which communications to target.[4]

Second, even if respondents could demonstrate that the targeting of their foreign contacts is imminent, respondents can only speculate as to whether the Government will seek to use § 1881a-authorized surveillance (rather than other methods) to do so. The Government has numerous other methods of conducting surveillance, none of which is challenged here. . .

Third, even if respondents could show that the Government will seek the Foreign Intelligence Surveillance Court's authorization to acquire the communications of respondents' foreign contacts under § 1881a, respondents can only speculate as to whether that court will authorize such surveillance. . .We decline to abandon our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors.

Fourth, even if the Government were to obtain the Foreign Intelligence Surveillance Court's approval to target respondents' foreign contacts under § 1881a, it is unclear whether the Government would succeed in acquiring the communications of respondents' foreign contacts. And fifth, even if the Government were to conduct surveillance of respondents' foreign contacts, respondents can only speculate as to whether *their own communications* with their foreign contacts would be incidentally acquired.

In sum, respondents' speculative chain of possibilities does not establish that injury based on potential future surveillance is certainly impending or is fairly traceable to § 1881a.

Respondents' alternative argument—namely, that they can establish standing based on the measures that they have undertaken to avoid § 1881a-authorized surveillance—fares no better. Respondents assert that they are suffering ongoing injuries that are fairly traceable to § 1881a because the risk of surveillance under § 1881a requires them to take costly and burdensome measures to protect the confidentiality of their communications. Respondents claim, for instance, that the threat of surveillance sometimes compels them to avoid certain e-mail and phone conversations, to "tal[k] in generalities rather than specifics," or to travel so that they can have in-person conversations.

Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm is unavailing—because the harm respondents seek to avoid is not certainly impending. In other words, respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending. Any ongoing injuries that respondents are suffering are not fairly traceable to § 1881a.

If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear. As Judge Raggi accurately noted, under the Second Circuit panel's reasoning, respondents could, "for the price of a plane ticket, ... transform their standing burden from one requiring a showing of actual or imminent ... interception to one requiring a showing that their subjective fear of such interception is not fanciful, irrational, or clearly unreasonable."). Thus, allowing respondents to bring this action based on costs they incurred in response to a speculative threat would be tantamount to accepting a repackaged version of respondents' first failed theory of standing.

For the reasons discussed above, respondents' self-inflicted injuries are not fairly traceable to the Government's purported activities under § 1881a, and their subjective fear of surveillance does not give rise to standing.

Respondents also suggest that they should be held to have standing because otherwise the constitutionality of § 1881a could not be challenged. It would be wrong, they maintain, to "insulate the government's surveillance activities from meaningful judicial review." Respondents' suggestion is both legally and factually incorrect. First, " '[t]he assumption that

if respondents have no standing to sue, no one would have standing, is not a reason to find standing.' " *Valley Forge Christian College* (1982).

Additionally, if the Government intends to use or disclose information obtained or derived from a § 1881a acquisition in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition. Thus, if the Government were to prosecute one of respondent-attorney's foreign clients using § 1881a-authorized surveillance, the Government would be required to make a disclosure. Although the foreign client might not have a viable Fourth Amendment claim, see, *e.g., United States v. Verdugo–Urquidez* (1990), it is possible that the monitoring of the target's conversations with his or her attorney would provide grounds for a claim of standing on the part of the attorney. Such an attorney would certainly have a stronger evidentiary basis for establishing standing than do respondents in the present case.

We hold that respondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm. We therefore reverse the judgment of the Second Circuit and remand the case for further proceedings consistent with this opinion.

Justice BREYER, with whom Justice GINSBURG, Justice SOTOMAYOR, and Justice KAGAN join, dissenting.

The plaintiffs' standing depends upon the likelihood that the Government, acting under the authority of 50 U.S.C. § 1881a, will harm them by intercepting at least some of their private, foreign, telephone, or e-mail conversations. In my view, this harm is not "speculative." Indeed it is as likely to take place as are most future events that commonsense inference and ordinary knowledge of human nature tell us will happen. This Court has often found the occurrence of similar future events sufficiently certain to support standing. I dissent from the Court's contrary conclusion.

No one here denies that the Government's interception of a private telephone or e-mail conversation amounts to an injury that is "concrete and particularized." Moreover, the plaintiffs, respondents here, seek as relief a judgment declaring unconstitutional (and enjoining enforcement of) a statutory provision authorizing those interceptions; and, such a judgment would redress the injury by preventing it. Thus, the basic question is whether the injury, *i.e.,* the interception, is "actual or imminent."

The addition of § 1881a in 2008 changed this prior law in three important ways. First, it eliminated the requirement that the Government describe to the court each specific target and identify each facility at which its surveillance would be directed, thus permitting surveillance on a programmatic, not necessarily individualized, basis. Second, it eliminated the requirement that a target be a "foreign power or an agent of a foreign power." Third, it diminished the court's authority to insist upon, and eliminated its authority to supervise, instance-specific privacy-intrusion minimization procedures (though the Government still must use court-approved general minimization procedures). Thus, using the authority of § 1881a, the Government can obtain court approval for its surveillance of electronic communications between places within the United States and targets in foreign territories by showing the court (1) that "a significant purpose of the acquisition is to obtain foreign intelligence information," and (2) that it will use general targeting and privacy-intrusion minimization procedures of a kind that the court had previously approved. § 1881a(g).

It is similarly important to understand the kinds of communications in which the plaintiffs say they engage and which they believe the Government will intercept. Plaintiff Scott McKay, for example, says in an affidavit (1) that he is a lawyer; (2) that he represented "Mr. Sami Omar Al–Hussayen, who was acquitted in June 2004 on terrorism charges"; (3) that he continues to represent "Mr. Al–Hussayen, who, in addition to facing criminal charges after

September 11, was named as a defendant in several civil cases"; (4) that he represents Khalid Sheik Mohammed, a detainee, "before the Military Commissions at Guantánamo Bay, Cuba"; (5) that in representing these clients he "communicate[s] by telephone and email with people outside the United States, including Mr. Al–Hussayen himself," "experts, investigators, attorneys, family members ... and others who are located abroad"; and (6) that prior to 2008 "the U.S. government had intercepted some 10,000 telephone calls and 20,000 email communications involving [his client] Al–Hussayen."

Another plaintiff, Sylvia Royce, says in her affidavit (1) that she is an attorney; (2) that she "represent[s] Mohammedou Ould Salahi, a prisoner who has been held at Guantánamo Bay as an enemy combatant"; (3) that, "[i]n connection with [her] representation of Mr. Salahi, [she] receive[s] calls from time to time from Mr. Salahi's brother, ... a university student in Germany"; and (4) that she has been told that the Government has threatened Salahi "that his family members would be arrested and mistreated if he did not cooperate."

A third plaintiff, Joanne Mariner, says in her affidavit (1) that she is a human rights researcher, (2) that "some of the work [she] do[es] involves trying to track down people who were rendered by the CIA to countries in which they were tortured"; (3) that many of those people "the CIA has said are (or were) associated with terrorist organizations"; and (4) that, to do this research, she "communicate[s] by telephone and e-mail with ... former detainees, lawyers for detainees, relatives of detainees, political activists, journalists, and fixers" "all over the world, including in Jordan, Egypt, Pakistan, Afghanistan, [and] the Gaza Strip."

Other plaintiffs, including lawyers, journalists, and human rights researchers, say in affidavits (1) that they have jobs that require them to gather information from foreigners located abroad; (2) that they regularly communicate electronically (*e.g.,* by telephone or e-mail) with foreigners located abroad; and (3) that in these communications they exchange "foreign intelligence information" as the Act defines it.

Several considerations, based upon the record along with commonsense inferences, convince me that there is a very high likelihood that Government, *acting under the authority of § 1881a,* will intercept at least some of the communications just described. First, the plaintiffs have engaged, and continue to engage, in electronic communications of a kind that the 2008 amendment, but not the prior Act, authorizes the Government to intercept. These communications include discussions with family members of those detained at Guantanamo, friends and acquaintances of those persons, and investigators, experts and others with knowledge of circumstances related to terrorist activities. These persons are foreigners located outside the United States. They are not "foreign power[s]" or "agent[s] of ... foreign power [s]." And the plaintiffs state that they exchange with these persons "foreign intelligence information," defined to include information that "relates to" "international terrorism" and "the national defense or the security of the United States."

Second, the plaintiffs have a strong *motive* to engage in, and the Government has a strong *motive* to listen to, conversations of the kind described. A lawyer representing a client normally seeks to learn the circumstances surrounding the crime (or the civil wrong) of which the client is accused. A fair reading of the affidavit of Scott McKay, for example, taken together with elementary considerations of a lawyer's obligation to his client, indicates that McKay will engage in conversations that concern what suspected foreign terrorists, such as his client, have done; in conversations that concern his clients' families, colleagues, and contacts; in conversations that concern what those persons (or those connected to them) have said and done, at least in relation to terrorist activities; in conversations that concern the political, social, and commercial environments in which the suspected terrorists have lived and worked; and so forth. Journalists and human rights workers have strong similar motives to conduct conversations of this kind.

At the same time, the Government has a strong motive to conduct surveillance of conversations that contain material of this kind. The Government, after all, seeks to learn as much as it can reasonably learn about suspected terrorists (such as those detained at Guantanamo), as well as about their contacts and activities, along with those of friends and family members.

Third, the Government's *past behavior* shows that it has sought, and hence will in all likelihood continue to seek, information about alleged terrorists and detainees through means that include surveillance of electronic communications. As just pointed out, plaintiff Scott McKay states that the Government (under the authority of the pre–2008 law) "intercepted some 10,000 telephone calls and 20,000 email communications involving [his client] Mr. Al–Hussayen."

Fourth, the Government has the *capacity* to conduct electronic surveillance of the kind at issue. To some degree this capacity rests upon technology available to the Government. . . .

Of course, to exercise this capacity the Government must have intelligence court authorization. But the Government rarely files requests that fail to meet the statutory criteria. See Letter from Ronald Weich, Assistant Attorney General, to Joseph R. Biden, Jr., 1 (Apr. 30, 2012) (In 2011, of the 1,676 applications to the intelligence court, two were withdrawn by the Government, and the remaining 1,674 were approved, 30 with some modification).

The upshot is that (1) similarity of content, (2) strong motives, (3) prior behavior, and (4) capacity all point to a very strong likelihood that the Government will intercept at least some of the plaintiffs' communications, including some that the 2008 amendment, § 1881a, but not the pre–2008 Act, authorizes the Government to intercept.

At the same time, nothing suggests the presence of some special factor here that might support a contrary conclusion. The Government does not deny that it has both the motive and the capacity to listen to communications of the kind described by plaintiffs. Nor does it describe any system for avoiding the interception of an electronic communication that happens to include a party who is an American lawyer, journalist, or human rights worker. One can, of course, always imagine some special circumstance that negates a virtual likelihood, no matter how strong. But the same is true about most, if not all, ordinary inferences about future events. Perhaps, despite pouring rain, the streets will remain dry (due to the presence of a special chemical). But ordinarily a party that seeks to defeat a strong natural inference must bear the burden of showing that some such special circumstance exists. And no one has suggested any such special circumstance here.

Consequently, we need only assume that the Government is doing its job (to find out about, and combat, terrorism) in order to conclude that there is a high probability that the Government will intercept at least some electronic communication to which at least some of the plaintiffs are parties. The majority is wrong when it describes the harm threatened plaintiffs as "speculative."

The majority more plausibly says that the plaintiffs have failed to show that the threatened harm is "*certainly impending*." But, as the majority appears to concede, *certainty* is not, and never has been, the touchstone of standing. The future is inherently uncertain. Yet federal courts frequently entertain actions for injunctions and for declaratory relief aimed at preventing future activities that are reasonably likely or highly likely, but not absolutely certain, to take place. And that degree of certainty is all that is needed to support standing here.

On still other occasions, recognizing that " 'imminence' is concededly a somewhat elastic concept," the Court has referred to, or used (sometimes along with "certainly impending") other phrases such as "reasonable probability" that suggest less than absolute, or literal certainty.

Taken together the case law uses the word "certainly" as if it emphasizes, rather than literally defines, the immediately following term " impending."

More important, the Court's holdings in standing cases show that standing exists here. The Court has often *found* standing where the occurrence of the relevant injury was far *less* certain than here. Consider a few, fairly typical, cases. Consider *Pennell*. A city ordinance forbade landlords to raise the rent charged to a tenant by more than 8 percent where doing so would work an unreasonably severe hardship on that tenant. A group of landlords sought a judgment declaring the ordinance unconstitutional. The Court held that, to have standing, the landlords had to demonstrate a " '*realistic danger of sustaining a direct injury* as a result of the statute's operation.' " It found that the landlords had done so by showing a likelihood of enforcement and a "probability," that the ordinance would make the landlords charge lower rents—even though the landlords had not shown (1) that they intended to raise the relevant rents to the point of causing unreasonably severe hardship; (2) that the tenants would challenge those increases; or (3) that the city's hearing examiners and arbitrators would find against the landlords. Here, even more so than in *Pennell,* there is a "*realistic danger* " that the relevant harm will occur.

In some standing cases, the Court has found that a reasonable probability of *future* injury comes accompanied with *present* injury that takes the form of reasonable efforts to mitigate the threatened effects of the future injury or to prevent it from occurring. Thus, in *Monsanto Co. v. Geertson Seed Farms* (2010), plaintiffs, a group of conventional alfalfa growers, challenged an agency decision to deregulate genetically engineered alfalfa. They claimed that deregulation would harm them because their neighbors would plant the genetically engineered seed, bees would obtain pollen from the neighbors' plants, and the bees would then (harmfully) contaminate their own conventional alfalfa with the genetically modified gene. The lower courts had found a "reasonable probability" that this injury would occur.

Without expressing views about that probability, we found standing because the plaintiffs would suffer present harm by trying to combat the threat. The plaintiffs, for example, "would have to conduct testing to find out whether and to what extent their crops have been contaminated." And they would have to take "measures to minimize the likelihood of potential contamination and to ensure an adequate supply of non-genetically-engineered alfalfa." We held that these "harms, which [the plaintiffs] will suffer even if their crops are not actually infected with" the genetically modified gene, "are sufficiently concrete to satisfy the injury-in-fact prong of the constitutional standing analysis."

Virtually identical circumstances are present here. Plaintiff McKay, for example, points out that, when he communicates abroad about, or in the interests of, a client (*e.g.,* a client accused of terrorism), he must "make an assessment" whether his "client's interests would be compromised" should the Government "acquire the communications." If so, he must either forgo the communication or travel abroad. ("I have had to take measures to protect the confidentiality of information that I believe is particularly sensitive," including "travel that is both time-consuming and expensive").

Since travel is expensive, since forgoing communication can compromise the client's interests, since McKay's assessment itself takes time and effort, this case does not differ significantly from *Monsanto.* And that is so whether we consider the plaintiffs' present necessary expenditure of time and effort as a separate concrete, particularized, imminent harm, or consider it as additional evidence that the future harm (an interception) is likely to occur.

While I express no view on the merits of the plaintiffs' constitutional claims, I do believe that at least some of the plaintiffs have standing to make those claims. I dissent, with respect, from the majority's contrary conclusion.

Notes

1. In some private civil cases, a plaintiff denied federal standing can bring the same action in a state court. And some plaintiffs would rather be in state court anyway. But one cannot sue the federal government in state court. So where, as here, the intended defendant is the federal government, a denial of standing is a dismissal of the case.
2. One point the majority raises in *Clapper* is that the use of 702 data in a criminal prosecution would require the disclosure of the fact that information was collected under 702 and also create a situation under which 702's constitutionality could be challenged. The below *Muhtorov* case is just such a challenge.

United States v. Muhtorov, 20 F.4th 558 (10th Cir. 2021)

Matheson, Circuit Judge.

Mr. Muhtorov arrived in the United States in 2007 as a political refugee from Uzbekistan and became a legal permanent resident. In 2009, he met Bakhtiyor Jumaev, a fellow Uzbekistan refugee with a similar background. The two became friends and developed a shared interest in the IJU [Islamic Jihad Union, a designated terrorist organization].

The government first became aware of Mr. Muhtorov's connection to the IJU through warrantless surveillance conducted under Section 702 of the Foreign Intelligence Surveillance Amendments Act of 2008. The Section 702 surveillance did not target Mr. Muhtorov. Rather, the government targeted a non-United States person living abroad, and in the process the government incidentally collected Mr. Muhtorov's communications with the target. The government then used those communications to support applications to surveil Mr. Muhtorov under the Foreign Intelligence Surveillance Act of 1978.

After securing approval under FISA, the government intercepted email communications between Mr. Muhtorov and an administrator of the IJU's official website beginning in 2011. In these communications, Mr. Muhtorov expressed his "support of the [IJU], his profession of allegiance to them, and his profession of wanting to provide whatever support he could to them." He discussed his intention to purchase portable satellite equipment and send $300 in cash, which he had received from Mr. Jumaev. He swore his "Bay'ah," or allegiance, to the IJU and said "he would do whatever is necessary for them or whatever they asked of him, even to the point of death."

In December 2011, Mr. Muhtorov told an ostensible IJU sympathizer—in reality, an informant for the Federal Bureau of Investigation ("FBI")—that he planned to travel to Turkey, and from there to join the IJU. On January 21, 2012, FBI agents arrested him at the Chicago airport as he was preparing to fly to Turkey on a one-way ticket. He was carrying nearly $3,000 in cash, two new iPhones, and a new iPad. His own phone contained videos showing combat against coalition forces, instructions on how to make explosive devices, and graphic images of jihadists beheading captured men.

Mr. Muhtorov argues the traditional FISA evidence that was presented at trial should have been suppressed as fruit of the poisonous tree because it was derived from the incidental collection of his communications during Section 702 surveillance. He challenges the Section 702 surveillance under the Fourth Amendment.

As enacted in 1978, FISA applied to communications "sent by or intended to be received by a . . . United States person who is in the United States" or "to or from a person in the United States . , , if such acquisition occurs in the United States." 50 U.S.C. § 1801(f)(1)–(2). FISA originally did not regulate electronic surveillance conducted abroad and directed at non-United States persons, even if the government happened to collect information from a communication with a United States person. And it did not apply to communications occurring entirely outside the country.

Congress enacted the FISA Amendments Act of 2008 ("FAA"), a major overhaul of FISA that set up two tracks for foreign intelligence surveillance. Under the FAA, traditional FISA continues to require a FISC-approved warrant for individual surveillance applications to target United States persons. The FAA added Section 702, 50 U.S.C. § 1881a, which provides the intelligence community with "additional authority to meet the challenges of modern technology and international terrorism."

[Section 702] broadens wiretap authority to allow warrantless surveillance of foreign targets reasonably believed to be overseas even if they may be communicating with people in the United States so long as the "purpose" is not to "target a particular, known person reasonably believed to be in the United States." The FISC must annually preapprove the procedures used to conduct the warrantless surveillance as reasonably designed to target foreigners outside the United States and to minimize the risk of surveilling United States persons. Congress also included a technical fix to allow wiretapping of communications that are routed through United States telecommunications switches if the target is a non-United States person located abroad.

Under Section 702, the government may compel telecommunications service providers located in the United States (including internet service providers and companies that maintain communications infrastructure) to provide emails or other electronic communications to, from, or about individuals the government believes are (a) not United States persons and (b) located abroad. Section 702 surveillance is subject to procedures relating to targeting, collection, minimization (including retention and dissemination), storage, and, beginning in 2018, querying databases containing Section 702 communications. In addition, the acquisition of foreign intelligence information must "be conducted in a manner consistent with the fourth amendment."

The Section 702 process works as follows:

Step One – Development of procedures

Targeting procedures must be "reasonably designed" to

> (A) ensure that any acquisition [of electronic communications] is limited to targeting persons reasonably believed to be located outside the United States; and
>
> (B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

These requirements implement Section 702's directive that the government may not "intentionally target" anyone located in the United States or a United States person located abroad. Likewise, the government "may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States." The targeting procedures are intended to prevent acquisition of the communications of United States persons or anyone in the United States.

Minimization "describes the manner in which the government processes communications after they have been collected and seeks to provide safeguards against the misuse of Section 702 information." Section 702 minimization procedures must "meet the definition of minimization procedures" for traditional FISA electronic surveillance or traditional FISA physical searches. They are "specific procedures . . . adopted by the Attorney General[ ] that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."

Querying involves searching through collected communications databases to find information relevant to a particular investigation or agency function. "[Q]uerying procedures do not govern the acquisition of information, but only the searches of already-acquired information contained in storage."

Step Two – Submission for FISC review

The AG and DNI [Director of National Intelligence] submit their targeting, minimization, and, beginning in 2018, querying procedures to the FISC for review. If the FISC finds the procedures "are consistent with the [statutory] requirements . . . and with the fourth amendment," the court enters an order approving them. "[J]udicial review of Section 702 functions as a form of programmatic pre-clearance." This pre-clearance is effective for one year. The AG and DNI must therefore submit Section 702 procedures to the FISC annually.

Step Three – Section 702 surveillance

After it receives FISC pre-clearance or an exigent-circumstances authorization, an intelligence agency "can begin surveilling individuals it seeks to target." "Section 702 surveillance usually begins when an agency 'tasks' a specific 'selector' or 'facility,' usually an e-mail address or telephone number." The AG and DNI may then "direct, in writing, an electronic communication service provider to . . . immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition" from that selector or facility. A service provider may challenge directives before the FISC, and the FISC may order compliance. The service provider may appeal the FISC's order.

The NSA operates two collection programs under Section 702: (1) "PRISM collection" and (2) "upstream collection."

If the government issues a directive to an internet service provider ("ISP"), such as Google or Microsoft, the resulting surveillance is known as "PRISM collection." Under PRISM, the government sends a certain identifier, such as an email address, to the ISP. The ISP then provides all communications sent to or from that identified email account. "PRISM, therefore, collects only the e-mails a given user sends from his or her account, and the e-mails he or she receives from others through that account."

For upstream collection, the government does not compel information from an ISP, but instead from the providers that control the underlying infrastructure over which telecommunications take place. Unlike PRISM, which collects only those communications that are sent from or to a target account hosted on a particular ISP, upstream collection casts a wider net not limited to a single ISP. It can capture communications that are *about* the target, even if the target is not the sender or recipient of the communication. The scope of upstream collection is thus much broader than PRISM.

"While the government cannot target U.S. persons or people located in the United States, it is permitted to acquire and in some cases retain and use communications in which a U.S. person is in contact with a target." This "incidental collection" concerns communications of a United States person or someone in the United States that are swept up through Section 702 surveillance because the person is communicating with a targeted non-United States person located abroad. Incidental collection "would occur under PRISM, for instance, if the NSA has targeted the e-mail address of a non-United States person in another country, and a United States person e-mails that targeted individual." In such situations the "ISP would be required to provide the NSA with any such e-mails as part of its compliance with a Section 702 directive targeting the non-United States party to the communication."

Step Four – Database storage

"Once communications are acquired under Section 702, they go into one or more databases at the NSA, CIA, and FBI." In theory, minimization procedures should lead to

deletion of incidentally collected communications that have no relevance to foreign intelligence. But deletion rarely happens. "Instead, those communications often remain in the agency's databases unreviewed until they are retrieved in response to a database query, or . . . deleted upon expiration of their retention period, without ever having been reviewed."

Thus, through Section 702, the government amasses large databases of communications, including communications to or from United States persons in the United States. And the government may later query these databases, such as for a name or email address. After-the-fact queries are sometimes called "backdoor searches."

Differences between Section 702 and traditional FISA

Section 702 differs from traditional FISA procedures in several key respects. First, traditional FISA requires a FISA warrant for a specific target supported by probable cause and specifying the nature and location of the facilities to be surveilled. But under Section 702, the FISC approves "procedures in advance, targeting non-United States persons located abroad as a category, and the government does not have to return to the FISC to seek approval before it undertakes surveillance of any specific individual or his or her accounts under those Section 702 procedures." Second, traditional FISA does not apply to targets located abroad. Section 702 authorizes surveillance of foreign targets and "eliminates the need for a traditional FISA order even if the surveillance (or other acquisition activity) targeting a non-U.S. person located abroad occurs inside the United States."

Challenge on Appeal

Mr. Muhtorov claims the government violated the Fourth Amendment when it incidentally collected his communications under Section 702. Because the government relied on those communications to obtain traditional FISA surveillance orders, he contends the resulting traditional FISA evidence introduced at trial should have been suppressed as fruit of the poisonous tree.

First, Mr. Muhtorov argues the government violated the Fourth Amendment when it incidentally collected his communications through Section 702 surveillance without a warrant. And even if a warrant was not required, he contends the surveillance was unreasonable.

Second, he asserts the government unconstitutionally queried Section 702 databases using identifiers associated with his name without a warrant. He contends that querying led to retrieval of communications or other information that were used to support the traditional FISA applications. But this is sheer speculation.

The government affirmatively represents that "the Section 702-derived evidence at issue was not obtained or derived from queries using terms associated with Muhtorov." The government further explains that "the Section 702 communications that the government described in the FISA applications were not the fruit of any queries using search terms associated with Muhtorov" and that "[t]he record therefore shows that the Section 702 information submitted to the FISC was not based on queries using terms associated with Muhtorov."

Our careful and independent review of the classified record, including the traditional FISA applications, confirms these representations are accurate. The record confirms that the relevant evidence did not arise from querying. We therefore do not address Mr. Muhtorov's second Fourth Amendment argument.

[O]ur analysis [of his first argument] proceeds in two steps. First, we must determine whether the absence of a warrant rendered the incidental collection of Mr. Muhtorov's communications "*per se* unreasonable." We determine that a warrant was not required, and the incidental collection was therefore not *per se* unreasonable. Second, we apply the *Maryland v.*

King reasonableness balancing test to the surveillance in this case. We conclude that it passes the reasonableness balancing test.

In rejecting Mr. Muhtorov's argument that the warrantless collection of his communications during Section 702 surveillance violated the Fourth Amendment, we join the Ninth Circuit in *United States v. Mohamud* (9th Cir. 2016), and the Second Circuit in *United States v. Hasbajrami* (2d Cir. 2019). Those courts found that similar warrantless incidental collection of a United States person's communications during the lawful Section 702 surveillance of a non-United States person did not violate the defendant's Fourth Amendment rights.

In the course of surveilling a non-United States person located abroad under Section 702, the government incidentally collected Mr. Muhtorov's communications. We conclude no warrant was required for (a) the Section 702 surveillance of the foreign target and (b) the incidental collection of Mr. Muhtorov's communications.

In *United States v. Verdugo-Urquidez* (1990), the Supreme Court held that the Fourth Amendment had "no application" to a search in Mexico of a citizen and resident of Mexico who had no voluntary attachment to the United States. The Court held the Fourth Amendment does not apply to foreign persons outside the United States, but only "to 'the people'"—a constitutional "term of art" that "refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."

The Court further explained that the Fourth Amendment "protect[s] the people of the United States against arbitrary action by their own Government" and "restrict[s] searches and seizures which might be conducted by the United States in domestic matters." But "it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States territory" or "to apply to activities of the United States directed against aliens in foreign territory." Applying the Fourth Amendment to law enforcement operations designed to protect national security "could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest."

Thus, "aliens receive constitutional protections [only] when they have come within the territory of the United States and developed substantial connections with this country."

We agree with *Mohamud* and *Hasbajrami*. When the target of Section 702 surveillance is a foreign national located abroad having no substantial connections with the United States, that target is not entitled to Fourth Amendment protections. Even if the instrumentalities of surveillance were located in the United States, the foreign target does not have Fourth Amendment protection because "what matters here is the location of the *target*, and not where the government literally obtained the electronic data." *Mohamud*. In this case, therefore, the government was not required to obtain a warrant before conducting the surveillance that targeted a non-United States person located abroad.

We turn to whether the government needed a warrant to collect Mr. Muhtorov's communications during the lawful Section 702 PRISM surveillance targeting a non-United States person located abroad. It did not.

The courts in *Mohamud* and *Hasbajrami* reached the same conclusion about similar incidental collections during lawful Section 702 surveillance. They relied on the "incidental overhear" doctrine developed in Title III wiretap cases. Although that doctrine lends support to our holding, we further rely on the "plain view" doctrine and the foreign surveillance context of the investigation

1) Plain view and incidental collection without a warrant

The incidental collection of Mr. Muhtorov's communications without a warrant during the course of otherwise lawful Section 702 surveillance was consistent with the justifications for the plain view doctrine.

The "initial intrusion" that brought the government into contact with Mr. Muhtorov's communications was "supported . . . by one of the recognized exceptions to the warrant requirement." It was lawful because, under *Verdugo-Urquidez*, no warrant is required to surveil foreigners located abroad.

It was then reasonable for the government to collect Mr. Muhtorov's communications during the otherwise lawful Section 702 surveillance. Once it was targeting the foreign national under PRISM, the government was lawfully "in" the two-way communications. In that position, it collected communications sent to and from the target. If Mr. Muhtorov happened to be the sender of a communication received by the target, or was the recipient of a communication sent by the target, then his communications could not be disentangled from the target's. The nature of PRISM surveillance and the commonsense notion that a communication involves at least two people means that Mr. Muhtorov's communications were necessarily in "plain view" of the government's Section 702 surveillance targeting the foreign national.

Moreover, it is impracticable to require the government to cease PRISM surveillance of a foreign target communicating with a United States person and immediately seek a traditional FISC warrant or Title III order. This is particularly so in cases like Mr. Muhtorov's, in which the "prevention or apprehension of terrorism suspects" is at the heart of the government's surveillance efforts. "Compulsory compliance with the warrant requirement would introduce an element of delay, thus frustrating the government's ability to collect information in a timely manner." *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act* (FISA Ct. Rev. 2008).

As the Second Circuit put it, "the overall practice of surveilling foreigners abroad of interest to the legitimate purpose of gathering foreign intelligence information may predictably lead to the interception of communications with United States persons." *Hasbajrami*. This predictability does not undermine the government's argument that no warrant was required for the incidental collection of Mr. Muhtorov's communications.

2) Foreign intelligence surveillance context – Section 702's statutory requirements

Two of Section 702's statutory requirements limited the scope of the incidental collection of Mr. Muhtorov's communications. Consistent with the plain view doctrine, these statutory limitations prevented the surveillance from becoming a "general exploratory search from one [communication] to another until something incriminating at last emerge[d]." *United States v. Carey* (10th Cir. 1999).

First, Section 702 surveillance must be intended to "acquire foreign intelligence information." 50 U.S.C. § 1881a(a). This requirement limits Section 702 surveillance to situations in which the government's power "to collect time-sensitive information" is paramount. *See In re Directives*. The statute's restriction to the foreign intelligence context, where the "government has the greatest need for speed, stealth, and secrecy," *United States v. Hung* (4th Cir. 1980), confines Section 702 surveillance to the "exigencies which justify its initiation"—that is, the foreign intelligence surveillance of foreigners located abroad, *see Horton v. California* (1990).

Second, Section 702 requires that surveillance be conducted "to minimize the acquisition and retention . . . of nonpublicly available information concerning unconsenting United States persons." 50 U.S.C. § 1801(h)(1). It forbids the government from "intentionally target[ing]" persons located in the United States, or outside the United States if the "purpose of such

acquisition is to target a particular" person in the United States. The minimization and targeting limitations on Section 702 surveillance are similar to the requirements described above that prevent plain view searches from becoming unreasonable general exploratory searches.

In sum, Section 702's statutory requirements—surveillance limited to foreign intelligence, and minimization and targeting limitations—helped to make the incidental collection of Mr. Muhtorov's communications "minimally intrusive[,] and [the] operational necessities render[ed] it the only practicable means of detecting certain types of crime." *See Arizona v. Hicks* (1987).

3) Incidental overhear

The Fourth Amendment principles discussed in the *United States v. Kahn* (1974), *United States v. Donovan* (1977), and later "incidental overhear" cases are rooted in the plain view doctrine and support our conclusion that no warrant was required.

First, plain view has been a mostly unspoken premise of the "incidental overhear" cases. *Kahn* and *Donovan* suggested that, once the surveilling officers obtained a Title III order and were lawfully listening to a conversation, they could seize a non-target's incriminating statements in "overheard" conversations without a warrant because the Fourth Amendment does not require "that all those likely to be overheard engaging in incriminating conversations be named." *Donovan*. Such a warrantless seizure would satisfy all three plain view requirements.

Second, the cases finding no warrant was required to seize communications of persons overheard on a wiretap are factually similar to the incidental collection of Mr. Muhtorov's communications. Both involve lawfully initiated electronic surveillance in which a non-target communicates with the target. Just as "surveillance under a [Title III] order that authorizes interception of calls of 'others as yet unknown' is not strictly limited to only those who are specifically named in the authorizing order," *United States v. Figueroa* (2d Cir. 1985), neither is lawfully initiated Section 702 surveillance that authorizes collection of a foreign target's communications strictly limited to collecting only that target's communications with non-United States persons.

Based on the foregoing, we find no warrant was required for the incidental collection of Mr. Muhtorov's communications.

Collection of Mr. Muhtorov's Communications Passed the Reasonableness Balancing Test

Although we find that the lack of a warrant did not render the incidental collection of Mr. Muhtorov's communications under Section 702 per se unreasonable, that does not end the analysis. The search must still be "reasonable in its scope and manner of execution." *Maryland v. King* (2013). The incidental collection of Mr. Muhtorov's communications was reasonable due largely to Section 702's provisions that constrained the government.

We balance "the promotion of legitimate governmental interests against the degree to which the search intrudes upon an individual's privacy." *Id*. The reasonableness balancing test is particularly concerned with ensuring that a search and seizure is "both limited and tailored reasonably to secure law enforcement needs while protecting privacy interests." *Illinois v. McArthur* (2001).

The Supreme Court has labeled "the Government's interest in combating terrorism . . . an urgent objective of the highest order." *Holder v. Humanitarian L. Project* (2010). This interest is implicated when the target of surveillance communicates with persons in the United States, such as Mr. Muhtorov, because "[t]he recruitment of persons inside the United States

or the placement of agents here to carry out terrorist attacks is one of the very threats that make it vital to surveil terrorist actors abroad." *Hasbajrami*.

We assume Mr. Muhtorov had a reasonable expectation of privacy in his communications that were monitored and intercepted through Section 702 surveillance. *See id.* (assuming the defendant had a privacy interest in his email communications and "that the government may not eavesdrop, without reasonable justification, on the conversations of United States persons (even abroad) with foreign nationals, simply because the United States person is interacting with a foreigner").

"An important component of the reasonableness inquiry is whether the FISC-approved targeting and minimization measures sufficiently protect the privacy interests of U.S. persons." *Mohamud; see, e.g.*, *In re Directives* (the minimization procedures under the PAA "serve . . . as a means of reducing the impact of incidental intrusions into the privacy on non-targeted United States persons").

Section 702 requires safeguards for privacy interests. The targeting and minimization procedures are designed to limit Section 702 surveillance only "to acquire foreign intelligence information." Section 702 requires the AG and DNI to develop procedures to comply with the statute's targeting, minimization, and querying requirements, and the FISC to review and approve these procedures. In addition, though intercepted communications might be voluminous, PRISM collection, unlike other surveillance programs, is more targeted and narrow in scope.

Under the totality of the circumstances, we find Mr. Muhtorov's privacy interest was "outweighed by the government's manifest need to monitor the communications of foreign agents of terrorist organizations operating abroad"—a need that "makes the incidental collection of communications between such foreigners and United States persons reasonable." *Hasbajrami*. The government has a strong interest in conducting foreign intelligence surveillance targeting those abroad.

The threat to the United States when foreign actors coordinate with and recruit United States persons bolsters the reasonableness of the incidental collection of United States persons' communications during lawful foreign intelligence surveillance directed at foreign nationals abroad. The "immediate objective" of the Section 702 surveillance here was to safeguard national security rather than "to generate evidence for law enforcement purposes." *See Ferguson v. City of Charleston* (2001).

In addition, the Section 702 program used to surveil Mr. Muhtorov is subject to targeting and minimization procedures and the overarching requirement that it be used for foreign intelligence gathering only. This is particularly true for PRISM collection.

LUCERO, Senior Judge, dissenting:

Based in part on the government's "affirmativ[e] represent[ation]" in its brief, the majority rejects one of Muhtorov's principal arguments on appeal—that the government violated the Fourth Amendment by querying § 702 data prior to the traditional FISA warrant application. In normal circumstances, appellate courts do not and should not rely on unsupported party assertions in their briefs to resolve disputes of fact. Given our affirmative duty to "place ourselves in the shoes of defense counsel, the very ones that cannot see the classified record, and act with a view to their interests," it is particularly extraordinary that my colleagues should blindly accept and rely on such an assertion. Although they assert that they have confirmed this representation through a "careful and independent view of the classified record," that they feel able to do so is surprising. The classified record is bereft of supporting evidence and the affirmative representation which the majority claims to have confirmed is directly contradicted by other government representations in its classified brief.

I agree with the majority's conclusion that the incidental *collection* of Muhtorov's communications with a target of § 702 surveillance is likely reasonable under the Fourth Amendment, but I find unacceptable the majority's decision to accept the government's assertion that no pre-warrant querying took place in light of the complete dearth of supporting evidence in the record. Querying stored § 702 data has "important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable." *United States v. Hasbajrami* (2d Cir. 2019). By accepting the government's bare assertion to resolve this dispute of fact, the majority avoids the thorny constitutional issues that querying presents. I would not blind myself to the constitutional implications raised by a "vast body of information" that may be "simply stored in a database, available for review by request from domestic law enforcement agencies solely on the speculative possibility that evidence of interest to agents investigating a particular individual might be found there." Unfortunately, the current record does not permit us to engage this question in a meaningful way.

Our inquiry, however, is almost immediately stymied by the record's silence on multiple facts that are crucial to the derivative evidence inquiry. Sidestepping our statutory duty to act as standby defense counsel, the majority accepts the government's unsupported assertions that "the Section 702-derived evidence at issue was not obtained or derived from queries using terms associated with Muhtorov." There is not one whit of evidence in the record to support this statement. To the contrary, the PCLOB [Privacy and Civil Liberties Oversight Board] Report, which provides the most-extensive declassified explanation of the § 702 program, indicates that the FBI almost certainly queried terms associated with Muhtorov prior to seeking a FISA warrant. Evidence in the classified record bolsters this conclusion.

The PCLOB Report explains that "whenever the FBI opens a new national security investigation or assessment, FBI personnel will query previously acquired information from a variety of sources, including Section 702, for information relevant to the investigation or assessment." The word choice is noteworthy—not "can" or "may," but the FBI *will* query stored § 702 information *whenever* the FBI opens a new national security investigation. As concerns Muhtorov, we know from the declassified *FBI Investigations and Operations Guide,* the unclassified record, and the government's brief, that the FBI opened a full investigation a legally significant period of time before it sought a traditional FISA warrant. It blinks reality to assert that, in this one instance, the FBI did not follow its standard operating procedure of querying § 702 data when opening a national security investigation. The majority does not engage with this contradiction, and there is no explanation in the record. Relying on an unsupported assertion in an appellate brief to resolve a disputed issue of fact is inappropriate in any circumstance, but to credit a factual assertion that is squarely rebutted by an official government report is unacceptable.

Understanding this, perhaps, the government tries to narrow our inquiry and contends that we need only be concerned with the specified number of communications that were included in the traditional FISA application—from which it appears the bulk of the evidence at trial derived. Because those communications were incidentally collected during the government's surveillance of the foreign target of the § 702 surveillance, the government argues, they were unaffected by any querying that may have occurred. But this argument subsumes the question we must resolve—was the decision to seek traditional FISA authority influenced by any querying of § 702 databases by the FBI using identifiers associated with Muhtorov? Or by information collected in other intelligence surveillance programs? And if it was the result of querying of § 702 databases, was the specific querying conducted reasonable under the Fourth Amendment under the facts of this case? After full review of the classified record, I cannot resolve this derivative evidence question.

Notes

1. Though we do not have access to the classified record, some of the dispute between the majority and dissent can be understood even absent that. The majority says that no queries using the defendant's name were used to produce evidence that formed the basis of the later FISA warrant application (and therefore of his much later prosecution). The dissent says that this does not mean that such queries were not run and did not aid investigators, only that investigators were able to cobble together a warrant application that did not directly use any of that material. Imagine that the dissent's concerns are correct and investigators did query Muhtorov and learn valuable information that either made him more of a target—encouraging future investigation on other fronts—or contextualized other available information. If so, how should that have affected the case?
2. The *Muhtorov* opinion relies on an earlier 2nd Circuit case, *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019). In January of 2025, the lower court in that case declassified an opinion that held that querying a 702 database is a separate Fourth Amendment event that requires a warrant, absent the foreign intelligence exception. *United States v. Hasbajrami*, 2025 WL 447498 (E.D.N.Y. Dec. 2, 2024). The court used *Riley* to inform its decision: just as law enforcement must obtain a warrant to search a lawfully seized cell phone, they must also obtain a warrant to search the Section 702 database. The court dismissed the argument that Section 702 minimization procedures render the warrant requirement unnecessary, reasoning that these minimization procedures are intended to protect U.S. persons in the same way a warrant does.

   The court held that the foreign intelligence exception to the warrant requirement does not apply because Government failed to meet its burden to show that its queries were beyond "garden-level" law enforcement use, and that its aims would have been hindered by the warrant requirement. Government offered little evidence detailing the nature and means of its queries. Even if the exception had applied, the court found the queries unreasonable under the Fourth Amendment. Citing *Carpenter*, the court found a high degree of intrusion by the Section 702 program, as individuals cannot opt out of its significant data collection. The sparse record provided by the government again offered little to weigh against that intrusion.

   The lower court's holding in *Hasbajrami*, however, was met with criticism. Writing in *Lawfare,* George Croner argued that the warrant requirement would severely burden the 702 program due to the sheer number of 702 queries conducted annually.[129] Specifically, a total of 69,207 queries of the Section 702 database using U.S. person identifiers were conducted in 2023, while the FISC only issued 352 Title I FISA orders, which require a showing of probable cause. Croner contended that the lower court failed to apply the "totality of the circumstances" standard to the Section 702 data collection and instead misapplied the law enforcement standard used in *Riley*. Croner asserted that when Section 702 querying is properly viewed through the lens of foreign intelligence gathering—and is limited by minimization procedures to queries "reasonably likely to retrieve foreign intelligence information"—it is reasonable under the Fourth Amendment without a warrant. Finally, Croner noted that Hasbajrami's attempt to join a terrorist organization abroad was thwarted by the Section 702 program—precisely the type of time-sensitive intelligence purpose that justifies the foreign intelligence exception.

[129] George Croner, *EDNY Opinion in Hasbajrami Undermines FISA 702*, Lawfare (March 31, 2025), https://www.lawfaremedia.org/article/edny-opinion-in-hasbajrami-undermines-fisa-702.

V. Substantive Due Process

A. The beginnings of constitutional decision privacy.....267
1) *Griswold*, history, and the start of the journey 268
Griswold v. Connecticut, 381 U.S. 479 (1965) 268
2) Abortion prior to *Dobbs* 271
3) Life, death, and gay rights 272
Washington v. Glucksberg, 521 U.S. 702 (1997) 272
Lawrence v. Texas, 539 U.S. 558 (2003) 276

B. Dobbs and the future of the right to decision privacy.....280
Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022) 280

C. The right to information privacy.....287
1) Foundations 287
Whalen v. Roe, 429 U.S. 589 (1977) 287
National Aeronautics and Space Administration v. Nelson, 562 U.S. 134 (2011) 292
2) Circuit level reactions to uncertainty 299
Dillard v. O'Kelley, 961 F.3d 1048 (8th Cir. 2020) 299
Sterling v. Borough of Minersville, 232 F.3d 190 (3rd Cir. 2000) 305

When people speak of privacy they can mean many things. When people speak of a constitutional right to privacy, however, they are thinking of the line of cases beginning with *Griswold v. Connecticut* and jutting out in strange protrusions to touch on the regulation of abortion, same-sex sexual relationships, same-sex legal relationships, and euthanasia. Depending on when one joins this conversation, one could end up with vastly different understandings of what the constitutional right to privacy "is really about."

In a way, this chapter is focused on exactly that question: what, if anything, is the right to privacy? Is it about intimate relationships, ideological and identity-related choices, bodily integrity, or some combination of the above? Or is it nothing at all—just a collection of convenient judicial fictions stuck under a common label?

Historically, the right has been divided into decisional and informational components. Decisional privacy is about the freedom to make certain decisions free from state interference. Informational privacy is about the freedom to make certain decisions without state monitoring. Since the right began in the decisional space, we will begin there as well.

A. The beginnings of constitutional decision privacy

The first case to clearly articulate the right to privacy was *Griswold v. Connecticut* (1965). As you will see, it cites a variety of early twentieth century cases as laying what it views as the foundation of the right. Consider the common thread—if you can find one—between those cases, *Griswold* itself, and what comes after. In particular, consider whether the right to privacy as articulated in *Griswold* is an individual right, belonging to particular people, or a relational right, about things people do together.

1) *Griswold*, history, and the start of the journey

Griswold v. Connecticut, 381 U.S. 479 (1965)

Mr. Justice DOUGLAS delivered the opinion of the Court.

Appellant Griswold is Executive Director of the Planned Parenthood League of Connecticut. Appellant Buxton is a licensed physician and a professor at the Yale Medical School who served as Medical Director for the League at its Center in New Haven—a center open and operating from November 1 to November 10, 1961, when appellants were arrested.

They gave information, instruction, and medical advice to *married persons* as to the means of preventing conception. They examined the wife and prescribed the best contraceptive device or material for her use. Fees were usually charged, although some couples were serviced free.

The statutes whose constitutionality is involved in this appeal are §§ 53—32 and 54—196 of the General Statutes of Connecticut (1958 rev.). The former provides:

> 'Any person who uses any drug, medicinal article or instrument for the purpose of preventing conception shall be fined not less than fifty dollars or imprisoned not less than sixty days nor more than one year or be both fined and imprisoned.'

Section 54—196 provides:

> 'Any person who assists, abets, counsels, causes, hires or commands another to commit any offense may be prosecuted and punished as if he were the principal offender.'

The appellants were found guilty as accessories and fined $100 each.

Coming to the merits, we are met with a wide range of questions that implicate the Due Process Clause of the Fourteenth Amendment. Overtones of some arguments suggest that *Lochner v. State of New York* (1905) should be our guide. But we decline that invitation. We do not sit as a super-legislature to determine the wisdom, need, and propriety of laws that touch economic problems, business affairs, or social conditions. This law, however, operates directly on an intimate relation of husband and wife and their physician's role in one aspect of that relation.

The association of people is not mentioned in the Constitution nor in the Bill of Rights. The right to educate a child in a school of the parents' choice—whether public or private or parochial—is also not mentioned. Nor is the right to study any particular subject or any foreign language. Yet the First Amendment has been construed to include certain of those rights.

By *Pierce v. Society of Sisters* (1925), the right to educate one's children as one chooses is made applicable to the States by the force of the First and Fourteenth Amendments. By *Meyer v. State of Nebraska* (1923), the same dignity is given the right to study the German language in a private school. In other words, the State may not, consistently with the spirit of the First Amendment, contract the spectrum of available knowledge. The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read and freedom of inquiry, freedom of thought, and freedom to teach—indeed the freedom of the entire university community. Without those peripheral rights the specific rights would be less secure. And so we reaffirm the principle of the *Pierce* and the *Meyer* cases.

In *NAACP v. State of Alabama* (1958), we protected the 'freedom to associate and privacy in one's associations,' noting that freedom of association was a peripheral First Amendment right. Disclosure of membership lists of a constitutionally valid association, we held, was invalid

'as entailing the likelihood of a substantial restraint upon the exercise by petitioner's members of their right to freedom of association.' In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion. In like context, we have protected forms of 'association' that are not political in the customary sense but pertain to the social, legal, and economic benefit of the members.

Those cases involved more than the 'right of assembly'—a right that extends to all irrespective of their race or ideology. The right of 'association,' like the right of belief, is more than the right to attend a meeting; it includes the right to express one's attitudes or philosophies by membership in a group or by affiliation with it or by other lawful means. Association in that context is a form of expression of opinion; and while it is not expressly included in the First Amendment its existence is necessary in making the express guarantees fully meaningful.

The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers 'in any house' in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: 'The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.'

The Fourth and Fifth Amendments were described in *Boyd v. United States* (1886) as protection against all governmental invasions 'of the sanctity of a man's home and the privacies of life.' We recently referred in *Mapp v. Ohio* (1961), to the Fourth Amendment as creating a 'right to privacy, no less important than any other right carefully and particularly reserved to the people.'

The present case, then, concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees. And it concerns a law which, in forbidding the use of contraceptives rather than regulating their manufacture or sale, seeks to achieve its goals by means having a maximum destructive impact upon that relationship. Such a law cannot stand in light of the familiar principle, so often applied by this Court, that a 'governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms.' Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship.

We deal with a right of privacy older than the Bill of Rights—older than our political parties, older than our school system. Marriage is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred. It is an association that promotes a way of life, not causes; a harmony in living, not political faiths; a bilateral loyalty, not commercial or social projects. Yet it is an association for as noble a purpose as any involved in our prior decisions.

Mr. Justice HARLAN, concurring in the judgment.

In my view, the proper constitutional inquiry in this case is whether this Connecticut statute infringes the Due Process Clause of the Fourteenth Amendment because the enactment violates basic values 'implicit in the concept of ordered liberty.' *Palko v. State of Connecticut* (1937). For reasons stated at length in my dissenting opinion in *Poe v. Ullman* (1961), I believe that it does. While the relevant inquiry may be aided by resort to one or more of the provisions

of the Bill of Rights, it is not dependent on them or any of their radiations. The Due Process Clause of the Fourteenth Amendment stands, in my opinion, on its own bottom.

Mr. Justice BLACK, with whom Mr. Justice STEWART joins, dissenting.

The Court talks about a constitutional 'right of privacy' as though there is some constitutional provision or provisions forbidding any law ever to be passed which might abridge the 'privacy' of individuals. But there is not. There are, of course, guarantees in certain specific constitutional provisions which are designed in part to protect privacy at certain times and places with respect to certain activities. Such, for example, is the Fourth Amendment's guarantee against 'unreasonable searches and seizures.' But I think it belittles that Amendment to talk about it as though it protects nothing but 'privacy.' The average man would very likely not have his feelings soothed any more by having his property seized openly than by having it seized privately and by stealth. He simply wants his property left alone. And a person can be just as much, if not more, irritated, annoyed and injured by an unceremonious public arrest by a policeman as he is by a seizure in the privacy of his office or home.

One of the most effective ways of diluting or expanding a constitutionally guaranteed right is to substitute for the crucial word or words of a constitutional guarantee another word or words, more or less flexible and more or less restricted in meaning. This fact is well illustrated by the use of the term 'right of privacy' as a comprehensive substitute for the Fourth Amendment's guarantee against 'unreasonable searches and seizures.' 'Privacy' is a broad, abstract and ambiguous concept which can easily be shrunken in meaning but which can also, on the other hand, easily be interpreted as a constitutional ban against many things other than searches and seizures. I have expressed the view many times that First Amendment freedoms, for example, have suffered from a failure of the courts to stick to the simple language of the First Amendment in construing it, instead of invoking multitudes of words substituted for those the Framers used. For these reasons I get nowhere in this case by talk about a constitutional 'right or privacy' as an emanation from one or more constitutional provisions. I like my privacy as well as the next one, but I am nevertheless compelled to admit that government has a right to invade it unless prohibited by some specific constitutional provision. For these reasons I cannot agree with the Court's judgment and the reasons it gives for holding this Connecticut law unconstitutional.

Mr. Justice STEWART, whom Mr. Justice BLACK joins, dissenting.

Since 1879 Connecticut has had on its books a law which forbids the use of contraceptives by anyone. I think this is an uncommonly silly law. As a practical matter, the law is obviously unenforceable, except in the oblique context of the present case. As a philosophical matter, I believe the use of contraceptives in the relationship of marriage should be left to personal and private choice, based upon each individual's moral, ethical, and religious beliefs. As a matter of social policy, I think professional counsel about methods of birth control should be available to all, so that each individual's choice can be meaningfully made. But we are not asked in this case to say whether we think this law is unwise, or even asinine. We are asked to hold that it violates the United States Constitution. And that I cannot do.

We are told that the Due Process Clause of the Fourteenth Amendment is not, as such, the 'guide' in this case. With that much I agree. There is no claim that this law, duly enacted by the Connecticut Legislature, is unconstitutionally vague. There is no claim that the appellants were denied any of the elements of procedural due process at their trial, so as to make their convictions constitutionally invalid. And, as the Court says, the day has long passed since the Due Process Clause was regarded as a proper instrument for determining 'the wisdom, need, and propriety' of state laws.

As to the First, Third, Fourth, and Fifth Amendments, I can find nothing in any of them to invalidate this Connecticut law, even assuming that all those Amendments are fully applicable against the States.

Notes

1. Everyone in *Griswold* agreed that the Connecticut law was bad. Both dissents mention it (Black's in an omitted section), and one even notes that one of the houses of the Connecticut legislature had recently voted to repeal the law. So here, unlike in some of the following cases, there is no ideological division on the wisdom of the law.
2. The majority cites two parental rights cases from the 1920s. In *Meyer v. Nebraska*, 262 U.S. 390 (1923), the Court ruled unconstitutional a law that prohibited the teaching of languages other than English before the eighth grade. The Court held that the liberties guaranteed by the Fourteenth Amendment did not merely include "freedom from bodily restraint but also the right . . . to acquire useful knowledge, [and] to marry, establish a home and bring up children . . . ." Just two years later in *Pierce v. Soc'y of the Sisters of the Holy Names of Jesus & Mary*, 268 U.S. 510, 534–35 (1925), the Court similarly held that a requirement that children attend public, as opposed to private, schools "unreasonably interferes with the liberty of parents and guardians to direct the upbringing and education of children." Given the history of the laws at issue, they were plainly intended to promote a particular form of American culture (Protestant, English-speaking) and discourage an alternative form (Catholic, German-speaking). The *Pierce* case is a particularly clear example of the Court refusing to allow a majority to impose ideological homogeneity on an objecting (and disliked) minority.[130]
3. Though the right to privacy has often been phrased in terms of the rights of women, it did not start there. The Court in *Griswold* did not focus on either the medical decision-making elements of contraceptive use or on the implications of the case for women's rights. In fact, the word "women" appears precisely once in the opinions, in Justice Black's dissent, and the word "wife" is only used five times, four of them as part of the phrase "husband and wife." Instead, particularly in the majority opinion, the emphasis was on the intrusion of the state into a *family's* private affairs. The switch from familial privacy to individual privacy appears to have occurred in *Eisenstadt v. Baird*, 405 U.S. 438 (1972), which struck down a law prohibiting the distribution of contraceptives to unmarried people. There, Justice Brennan wrote that "[i]f the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child." Notably, he wrote those words fully aware that abortion was the next major privacy issue for the Court.

The contraception cases mark out a zone of autonomy into which the government cannot intrude. In both *Griswold* and *Eisenstadt*, the zone is defined around family interests. However, as seen in *Eisenstadt*, family is being interpreted broadly enough that it is sensible for Justice Brennan to speak of the rights of an "individual" to make the childbearing decision. The contraception cases are also notable for expanding privacy beyond the realm of political expression. Unlike in *Meyer* and *Pierce*, there is no undercurrent of protecting ideological minorities in *Griswold*.

2) Abortion prior to *Dobbs*

This trend toward privacy as an individual right was further developed as the Court considered abortion rights eight years after *Griswold* in *Roe v. Wade*, 410 U.S. 113 (1973). Speaking for the Court in *Roe*, Justice Blackmun stated that the right to privacy "is broad enough to encompass a woman's decision whether or not to terminate her pregnancy." In reaching this conclusion, Blackmun cited the same lines of cases that had buttressed the

[130] *See generally*, PAULA ABRAMS, CROSS PURPOSES: PIERCE V. SOCIETY OF SISTERS AND THE STRUGGLE OVER COMPULSORY PUBLIC EDUCATION (Univ. of Mich. 2009).

Griswold decision, with the added support of both *Griswold* itself and a line of cases extending due process protection into areas of marriage and procreation.[131]

Unlike in *Griswold*, however, the experiences and interests of the pregnant woman were central in *Roe*. The Court noted that the woman's health, both psychological and physical, would be substantially affected by the continuation of her pregnancy, and that maternity may "force upon the woman a distressful life in future." Further, if the woman was unmarried, she might face "the additional difficulties and continuing stigma of unwed motherhood." Given these substantial privacy costs, the state could only regulate in this area where it had a "compelling" interest.

Roe's focus on individual autonomy and the standards of medical practice actually distinguishes it somewhat from the prior privacy cases. In *Pierce* and *Griswold*, the privacy interest being burdened was fundamentally interpersonal; the state was stepping between two people. Here, the privacy interest is individuated. The right being impinged belongs to an individual woman, alone, and the question is the extent to which the state can control her personal decision-making.

Even in *Roe* itself, the Court recognized that the right to privacy was "not absolute" in this context and that "at some point the state interests as to protection of health, medical standards, and prenatal life, become dominant." In *Planned Parenthood of Southeastern Pennsylvania v. Casey*, 505 U.S. 833 (1992), the Court held that regulations that did not place an "undue burden" on the woman's right to choose were constitutionally permissible. Thus, the Court upheld parental notification and consent provisions for minors; waiting periods; some regulations of abortion facilities themselves; and a rigorous informed-consent requirement. Still, it struck down a spousal notification requirement, observing that "[t]he Constitution protects individuals, men and women alike, from unjustified state interference, even when that interference is enacted into law for the benefit of their spouses." The requirement therefore imposed an "undue burden."

3) Life, death, and gay rights

Law develops chronologically rather than thematically. Although the abortion story from *Roe* and *Casey* will continue in *Dobbs*, the doctrine seen in *Dobbs* has less to do with either of those cases and more to do with *Lawrence v. Texas* (2003), which concerned same-sex sexual relationships, and the general debate over substantive due process. We therefore need to consider, first, the substantive due process test developed in *Washington v. Glucksberg* (1997) and, second, the core interests identified by the Court in *Lawrence v. Texas* before continuing the abortion story in *Dobbs*.

Washington v. Glucksberg, 521 U.S. 702 (1997)

Chief Justice REHNQUIST delivered the opinion of the Court.

The question presented in this case is whether Washington's prohibition against "caus[ing]" or "aid[ing]" a suicide offends the Fourteenth Amendment to the United States Constitution. We hold that it does not.

It has always been a crime to assist a suicide in the State of Washington. In 1854, Washington's first Territorial Legislature outlawed "assisting another in the commission of self-murder." Today, Washington law provides: "A person is guilty of promoting a suicide attempt when he knowingly causes or aids another person to attempt suicide."

---

[131] *Loving v. Virginia*, 388 U.S. 1, 12 (1967) (marriage); *Skinner v. Oklahoma*, 316 U.S. 535, 541–542 (1942) (procreation).

Petitioners in this case are doctors [who] occasionally treat terminally ill, suffering patients, and declare that they would assist these patients in ending their lives if not for Washington's assisted-suicide ban.

The plaintiffs asserted "the existence of a liberty interest protected by the Fourteenth Amendment which extends to a personal choice by a mentally competent, terminally ill adult to commit physician-assisted suicide."

We begin, as we do in all due process cases, by examining our Nation's history, legal traditions, and practices. In almost every State—indeed, in almost every western democracy—it is a crime to assist a suicide. The States' assisted-suicide bans are not innovations. Rather, they are longstanding expressions of the States' commitment to the protection and preservation of all human life. Indeed, opposition to and condemnation of suicide—and, therefore, of assisting suicide—are consistent and enduring themes of our philosophical, legal, and cultural heritages.

More specifically, for over 700 years, the Anglo-American common-law tradition has punished or otherwise disapproved of both suicide and assisting suicide. In the 13th century, Henry de Bracton, one of the first legal-treatise writers, observed that "[j]ust as a man may commit felony by slaying another so may he do so by slaying himself." 2 Bracton on Laws and Customs of England 423. The real and personal property of one who killed himself to avoid conviction and punishment for a crime were forfeit to the King; however, thought Bracton, "if a man slays himself in weariness of life or because he is unwilling to endure further bodily pain . . . [only] his movable goods [were] confiscated." Thus, "[t]he principle that suicide of a sane person, for whatever reason, was a punishable felony was . . . introduced into English common law."

For the most part, the early American Colonies adopted the common-law approach. Over time, however, the American Colonies abolished these harsh common-law penalties. William Penn abandoned the criminal-forfeiture sanction in Pennsylvania in 1701, and the other Colonies (and later, the other States) eventually followed this example.

Nonetheless, although States moved away from Blackstone's treatment of suicide, courts continued to condemn it as a grave public wrong. That suicide remained a grievous, though nonfelonious, wrong is confirmed by the fact that colonial and early state legislatures and courts did not retreat from prohibiting assisting suicide.

Though deeply rooted, the States' assisted-suicide bans have in recent years been reexamined and, generally, reaffirmed. Because of advances in medicine and technology, Americans today are increasingly likely to die in institutions, from chronic illnesses. Public concern and democratic action are therefore sharply focused on how best to protect dignity and independence at the end of life, with the result that there have been many significant changes in state laws and in the attitudes these laws reflect. Many States, for example, now permit "living wills," surrogate health-care decisionmaking, and the withdrawal or refusal of life-sustaining medical treatment. At the same time, however, voters and legislators continue for the most part to reaffirm their States' prohibitions on assisting suicide.

The Due Process Clause guarantees more than fair process, and the "liberty" it protects includes more than the absence of physical restraint. The Clause also provides heightened protection against government interference with certain fundamental rights and liberty interests. In a long line of cases, we have held that, in addition to the specific freedoms protected by the Bill of Rights, the "liberty" specially protected by the Due Process Clause includes the rights to marry, to have children, to direct the education and upbringing of one's children, to marital privacy, to use contraception, to bodily integrity, and to abortion. We have also assumed, and strongly suggested, that the Due Process Clause protects the traditional right to refuse unwanted lifesaving medical treatment.

But we "ha[ve] always been reluctant to expand the concept of substantive due process because guideposts for responsible decisionmaking in this unchartered area are scarce and open-ended." By extending constitutional protection to an asserted right or liberty interest, we, to a great extent, place the matter outside the arena of public debate and legislative action. We must therefore "exercise the utmost care whenever we are asked to break new ground in this field," lest the liberty protected by the Due Process Clause be subtly transformed into the policy preferences of the Members of this Court.

Our established method of substantive-due-process analysis has two primary features: First, we have regularly observed that the Due Process Clause specially protects those fundamental rights and liberties which are, objectively, "deeply rooted in this Nation's history and tradition," *Snyder v. Massachusetts* (1934) ("so rooted in the traditions and conscience of our people as to be ranked as fundamental"), and "implicit in the concept of ordered liberty," such that "neither liberty nor justice would exist if they were sacrificed," *Palko v. Connecticut* (1937). Second, we have required in substantive-due-process cases a "careful description" of the asserted fundamental liberty interest. Our Nation's history, legal traditions, and practices thus provide the crucial "guideposts for responsible decisionmaking," that direct and restrain our exposition of the Due Process Clause. As we stated recently in *Reno v. Flores* (1993), the Fourteenth Amendment "forbids the government to infringe . . . 'fundamental' liberty interests *at all,* no matter what process is provided, unless the infringement is narrowly tailored to serve a compelling state interest."

We now inquire whether this asserted right has any place in our Nation's traditions. Here we are confronted with a consistent and almost universal tradition that has long rejected the asserted right, and continues explicitly to reject it today, even for terminally ill, mentally competent adults. To hold for respondents, we would have to reverse centuries of legal doctrine and practice, and strike down the considered policy choice of almost every State. See *Jackman v. Rosenbaum Co.* (1922) ("If a thing has been practised for two hundred years by common consent, it will need a strong case for the Fourteenth Amendment to affect it"); *Flores* ("The mere novelty of such a claim is reason enough to doubt that 'substantive due process' sustains it").

Respondents contend, however, that the liberty interest they assert is consistent with this Court's substantive-due-process line of cases, if not with this Nation's history and practice. Pointing to *Planned Parenthood of Southeastern Pa. v. Casey* (1992) and *Cruzan v. Director, Mo. Dep't of Health* (1990), respondents read our jurisprudence in this area as reflecting a general tradition of "self-sovereignty," and as teaching that the "liberty" protected by the Due Process Clause includes "basic and intimate exercises of personal autonomy."

In *Cruzan,* we considered whether Nancy Beth Cruzan, who had been severely injured in an automobile accident and was in a persistive vegetative state, "ha[d] a right under the United States Constitution which would require the hospital to withdraw life-sustaining treatment" at her parents' request. We began with the observation that "[a]t common law, even the touching of one person by another without consent and without legal justification was a battery." We then discussed the related rule that "informed consent is generally required for medical treatment." After reviewing a long line of relevant state cases, we concluded that "the common-law doctrine of informed consent is viewed as generally encompassing the right of a competent individual to refuse medical treatment." Therefore, "for purposes of [that] case, we assume[d] that the United States Constitution would grant a competent person a constitutionally protected right to refuse lifesaving hydration and nutrition."

The right assumed in *Cruzan,* however, was not simply deduced from abstract concepts of personal autonomy. Given the common-law rule that forced medication was a battery, and the long legal tradition protecting the decision to refuse unwanted medical treatment, our assumption was entirely consistent with this Nation's history and constitutional traditions. The decision to commit suicide with the assistance of another may be just as personal and profound

as the decision to refuse unwanted medical treatment, but it has never enjoyed similar legal protection. Indeed, the two acts are widely and reasonably regarded as quite distinct.

The history of the law's treatment of assisted suicide in this country has been and continues to be one of the rejection of nearly all efforts to permit it. The Constitution also requires, however, that Washington's assisted-suicide ban be rationally related to legitimate government interests. This requirement is unquestionably met here.

First, Washington has an "unqualified interest in the preservation of human life." Those who attempt suicide—terminally ill or not—often suffer from depression or other mental disorders. Research indicates, however, that many people who request physician-assisted suicide withdraw that request if their depression and pain are treated. The State also has an interest in protecting the integrity and ethics of the medical profession. [T]he American Medical Association, like many other medical and physicians' groups, has concluded that "[p]hysician-assisted suicide is fundamentally incompatible with the physician's role as healer." Next, the State has an interest in protecting vulnerable groups—including the poor, the elderly, and disabled persons—from abuse, neglect, and mistakes. [AUTH Note: each of these points is developed at length in the full opinion]

We need not weigh exactingly the relative strengths of these various interests. They are unquestionably important and legitimate, and Washington's ban on assisted suicide is at least reasonably related to their promotion and protection.

Notes

1. The right to die debates of the 1990s—which cooled subsequently, perhaps because a number of states have recognized the right on their own—provide some boundary markers for the right of privacy. Contrasting *Glucksberg* and the earlier *Cruzan* case on refusing treatment, the Court differentiates between respecting a person's wish to refuse future medical treatment, even when that refusal would result in their death, and their wish to have active medical intervention that would result in their death. Does this difference feel meaningful to you? If refusal of a feeding tube will result in death in three days, is there any reason to deny an injection that will result in death in three minutes? If not, how far can you comfortably push this principle?
2. The general theme of the *Glucksberg* test is that the Court is extremely reluctant to recognize new rights for decisional privacy. And, when it recognizes rights, it does not want to construe them broadly or vaguely.

To understand the next case, we must step back into the 1980s. In *Bowers v. Hardwick*, 478 U.S. 186 (1986) the Court upheld the constitutionality of a Georgia sodomy law criminalizing oral and anal sex in private between consenting adults. The facts of the case concerned a same-sex pair, but the law did not differentiate on those grounds. Justice White, writing for the Court, said that the Constitution did not confer "a fundamental right to engage in homosexual sodomy." A concurring opinion by Chief Justice Warren E. Burger cited the "ancient roots" of prohibitions against homosexual sex. Burger concluded, "To hold that the act of homosexual sodomy is somehow protected as a fundamental right would be to cast aside millennia of moral teaching."

In a way, *Bowers* is entirely consistent with the later *Glucksberg* case. There was nothing in the prior case law protecting particular sex acts from government regulation and nothing in it regarding same-sex couples or intimacy. There was a strong historical tradition opposed to the right. Therefore, finding a right in support of the defendants would have required construing the liberty interests protected by the Fourteenth Amendment broadly, which the Court was reluctant to do. Notably, however, *Bowers* was decided 5-4. The dissenters would have been willing to make that leap. And, almost two decades later, a majority did so.

Lawrence v. Texas, 539 U.S. 558 (2003)

Justice KENNEDY delivered the opinion of the Court.

Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct. The instant case involves liberty of the person both in its spatial and in its more transcendent dimensions.

I

The question before the Court is the validity of a Texas statute making it a crime for two persons of the same sex to engage in certain intimate sexual conduct.

In Houston, Texas, officers of the Harris County Police Department were dispatched to a private residence in response to a reported weapons disturbance. They entered an apartment where one of the petitioners, John Geddes Lawrence, resided. The right of the police to enter does not seem to have been questioned. The officers observed Lawrence and another man, Tyron Garner, engaging in a sexual act. The two petitioners were arrested, held in custody overnight, and charged and convicted before a Justice of the Peace.

The complaints described their crime as "deviate sexual intercourse, namely anal sex, with a member of the same sex (man)." The applicable state law is Tex. Penal Code Ann. § 21.06(a) (2003). It provides: "A person commits an offense if he engages in deviate sexual intercourse with another individual of the same sex." The statute defines "[d]eviate sexual intercourse" as follows:

> "(A) any contact between any part of the genitals of one person and the mouth or anus of another person; or
>
> (B) the penetration of the genitals or the anus of another person with an object."

II

We conclude the case should be resolved by determining whether the petitioners were free as adults to engage in the private conduct in the exercise of their liberty under the Due Process Clause of the Fourteenth Amendment to the Constitution. For this inquiry we deem it necessary to reconsider the Court's holding in *Bowers v. Hardwick* (1986).

The Court began its substantive discussion in *Bowers* as follows: "The issue presented is whether the Federal Constitution confers a fundamental right upon homosexuals to engage in sodomy and hence invalidates the laws of the many States that still make such conduct illegal and have done so for a very long time." That statement, we now conclude, discloses the Court's own failure to appreciate the extent of the liberty at stake. To say that the issue in *Bowers* was simply the right to engage in certain sexual conduct demeans the claim the individual put forward, just as it would demean a married couple were it to be said marriage is simply about the right to have sexual intercourse. The laws involved in *Bowers* and here are, to be sure, statutes that purport to do no more than prohibit a particular sexual act. Their penalties and purposes, though, have more far-reaching consequences, touching upon the most private human conduct, sexual behavior, and in the most private of places, the home. The statutes do seek to control a personal relationship that, whether or not entitled to formal recognition in the law, is within the liberty of persons to choose without being punished as criminals.

At the outset it should be noted that there is no longstanding history in this country of laws directed at homosexual conduct as a distinct matter. Beginning in colonial times there were prohibitions of sodomy derived from the English criminal laws passed in the first instance

by the Reformation Parliament of 1533. The English prohibition was understood to include relations between men and women as well as relations between men and men. This does not suggest approval of homosexual conduct. It does tend to show that this particular form of conduct was not thought of as a separate category from like conduct between heterosexual persons.

Laws prohibiting sodomy do not seem to have been enforced against consenting adults acting in private. A substantial number of sodomy prosecutions and convictions for which there are surviving records were for predatory acts against those who could not or did not consent, as in the case of a minor or the victim of an assault.

It was not until the 1970s that any State singled out same-sex relations for criminal prosecution, and only nine States have done so. Post-*Bowers* even some of these States did not adhere to the policy of suppressing homosexual conduct. Over the course of the last decades, States with same-sex prohibitions have moved toward abolishing them.

In summary, the historical grounds relied upon in *Bowers* are more complex than the majority opinion and the concurring opinion by Chief Justice Burger indicate. Their historical premises are not without doubt and, at the very least, are overstated.

It must be acknowledged, of course, that the Court in *Bowers* was making the broader point that for centuries there have been powerful voices to condemn homosexual conduct as immoral. The condemnation has been shaped by religious beliefs, conceptions of right and acceptable behavior, and respect for the traditional family. For many persons these are not trivial concerns but profound and deep convictions accepted as ethical and moral principles to which they aspire and which thus determine the course of their lives. These considerations do not answer the question before us, however. The issue is whether the majority may use the power of the State to enforce these views on the whole society through operation of the criminal law. "Our obligation is to define the liberty of all, not to mandate our own moral code." *Planned Parenthood of Southeastern Pa. v. Casey* (1992).

In all events we think that our laws and traditions in the past half century are of most relevance here. These references show an emerging awareness that liberty gives substantial protection to adult persons in deciding how to conduct their private lives in matters pertaining to sex. "[H]istory and tradition are the starting point but not in all cases the ending point of the substantive due process inquiry." *County of Sacramento v. Lewis* (1998) (KENNEDY, J., concurring).

Of even more importance, almost five years before *Bowers* was decided the European Court of Human Rights considered a case with parallels to *Bowers* and to today's case. An adult male resident in Northern Ireland alleged he was a practicing homosexual who desired to engage in consensual homosexual conduct. The court held that the laws proscribing the conduct were invalid under the European Convention on Human Rights. *Dudgeon v. United Kingdom,* 45 Eur. Ct. H.R. (1981). Authoritative in all countries that are members of the Council of Europe (21 nations then, 45 nations now), the decision is at odds with the premise in *Bowers* that the claim put forward was insubstantial in our Western civilization.

In our own constitutional system the deficiencies in *Bowers* became even more apparent in the years following its announcement. The 25 States with laws prohibiting the relevant conduct referenced in the *Bowers* decision are reduced now to 13, of which 4 enforce their laws only against homosexual conduct. In those States where sodomy is still proscribed, whether for same-sex or heterosexual conduct, there is a pattern of nonenforcement with respect to consenting adults acting in private. The State of Texas admitted in 1994 that as of that date it had not prosecuted anyone under those circumstances. *State v. Morales* (Tex. 1994).

Two principal cases decided after *Bowers* cast its holding into even more doubt. In *Casey*, the Court reaffirmed the substantive force of the liberty protected by the Due Process Clause.

The *Casey* decision again confirmed that our laws and tradition afford constitutional protection to personal decisions relating to marriage, procreation, contraception, family relationships, child rearing, and education. Persons in a homosexual relationship may seek autonomy for these purposes, just as heterosexual persons do. The decision in *Bowers* would deny them this right.

Equality of treatment and the due process right to demand respect for conduct protected by the substantive guarantee of liberty are linked in important respects, and a decision on the latter point advances both interests. If protected conduct is made criminal and the law which does so remains unexamined for its substantive validity, its stigma might remain even if it were not enforceable as drawn for equal protection reasons. When homosexual conduct is made criminal by the law of the State, that declaration in and of itself is an invitation to subject homosexual persons to discrimination both in the public and in the private spheres. The central holding of *Bowers* has been brought in question by this case, and it should be addressed. Its continuance as precedent demeans the lives of homosexual persons.

Bowers was not correct when it was decided, and it is not correct today. It ought not to remain binding precedent. *Bowers* should be and now is overruled.

The present case does not involve minors. It does not involve persons who might be injured or coerced or who are situated in relationships where consent might not easily be refused. It does not involve public conduct or prostitution. It does not involve whether the government must give formal recognition to any relationship that homosexual persons seek to enter. The case does involve two adults who, with full and mutual consent from each other, engaged in sexual practices common to a homosexual lifestyle. The petitioners are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their private sexual conduct a crime. Their right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government. "It is a promise of the Constitution that there is a realm of personal liberty which the government may not enter." *Casey*. The Texas statute furthers no legitimate state interest which can justify its intrusion into the personal and private life of the individual.

Justice O'CONNOR, concurring in the judgment.

The Court today overrules *Bowers v. Hardwick* (1986). I joined *Bowers,* and do not join the Court in overruling it. Nevertheless, I agree with the Court that Texas' statute banning same-sex sodomy is unconstitutional. Rather than relying on the substantive component of the Fourteenth Amendment's Due Process Clause, as the Court does, I base my conclusion on the Fourteenth Amendment's Equal Protection Clause.

Moral disapproval of a group cannot be a legitimate governmental interest under the Equal Protection Clause because legal classifications must not be "drawn for the purpose of disadvantaging the group burdened by the law." Texas' invocation of moral disapproval as a legitimate state interest proves nothing more than Texas' desire to criminalize homosexual sodomy.

That this law as applied to private, consensual conduct is unconstitutional under the Equal Protection Clause does not mean that other laws distinguishing between heterosexuals and homosexuals would similarly fail under rational basis review. Texas cannot assert any legitimate state interest here, such as national security or preserving the traditional institution of marriage. Unlike the moral disapproval of same-sex relations—the asserted state interest in this case—other reasons exist to promote the institution of marriage beyond mere moral disapproval of an excluded group.

A law branding one class of persons as criminal based solely on the State's moral disapproval of that class and the conduct associated with that class runs contrary to the values of the Constitution and the Equal Protection Clause, under any standard of review. I therefore

concur in the Court's judgment that Texas' sodomy law banning "deviate sexual intercourse" between consenting adults of the same sex, but not between consenting adults of different sexes, is unconstitutional.

Justice SCALIA, with whom THE CHIEF JUSTICE and Justice THOMAS join, dissenting.

"Liberty finds no refuge in a jurisprudence of doubt." *Planned Parenthood of Southeastern Pa. v. Casey* (1992). That was the Court's sententious response, barely more than a decade ago, to those seeking to overrule *Roe v. Wade* (1973). The Court's response today, to those who have engaged in a 17–year crusade to overrule *Bowers v. Hardwick* (1986), is very different. The need for stability and certainty presents no barrier.

Countless judicial decisions and legislative enactments have relied on the ancient proposition that a governing majority's belief that certain sexual behavior is "immoral and unacceptable" constitutes a rational basis for regulation. *See, e.g.*, *Williams v. Pryor* (11th Cir. 2001) (citing *Bowers* in upholding Alabama's prohibition on the sale of sex toys on the ground that "[t]he crafting and safeguarding of public morality . . . indisputably is a legitimate government interest under rational basis scrutiny"); *Holmes v. California Army National Guard* (9th Cir. 1997) (relying on *Bowers* in upholding the federal statute and regulations banning from military service those who engage in homosexual conduct); *Owens v. State* (1999) (relying on *Bowers* in holding that "a person has no constitutional right to engage in sexual intercourse, at least outside of marriage"); *Sherman v. Henry* (Tex. 1996) (relying on *Bowers* in rejecting a claimed constitutional right to commit adultery). We ourselves relied extensively on *Bowers* when we concluded, in *Barnes v. Glen Theatre, Inc.* (1991), that Indiana's public indecency statute furthered "a substantial government interest in protecting order and morality," (plurality opinion). State laws against bigamy, same-sex marriage, adult incest, prostitution, masturbation, adultery, fornication, bestiality, and obscenity are likewise sustainable only in light of *Bowers*' validation of laws based on moral choices. Every single one of these laws is called into question by today's decision; the Court makes no effort to cabin the scope of its decision to exclude them from its holding. The impossibility of distinguishing homosexuality from other traditional "morals" offenses is precisely why *Bowers* rejected the rational-basis challenge.

Our opinions applying the doctrine known as "substantive due process" hold that the Due Process Clause prohibits States from infringing *fundamental* liberty interests, unless the infringement is narrowly tailored to serve a compelling state interest. We have held repeatedly, in cases the Court today does not overrule, that *only* fundamental rights qualify for this so-called "heightened scrutiny" protection—that is, rights which are "'deeply rooted in this Nation's history and tradition.'" All other liberty interests may be abridged or abrogated pursuant to a validly enacted state law if that law is rationally related to a legitimate state interest.

In any event, an "emerging awareness" is by definition not "deeply rooted in this Nation's history and tradition[s]," as we have said "fundamental right" status requires. Constitutional entitlements do not spring into existence because some States choose to lessen or eliminate criminal sanctions on certain behavior. Much less do they spring into existence, as the Court seems to believe, because *foreign nations* decriminalize conduct.

Today's opinion is the product of a Court, which is the product of a law-profession culture, that has largely signed on to the so-called homosexual agenda, by which I mean the agenda promoted by some homosexual activists directed at eliminating the moral opprobrium that has traditionally attached to homosexual conduct.

Notes

1. Justice Scalia writes that "State laws against bigamy, same-sex marriage, adult incest, prostitution, masturbation, adultery, fornication, bestiality, and obscenity" are only sustainable if the state is allowed to legislate moral choices. Which of these laws are sustainable in light of the majority in *Lawrence*? Can a state enforce a law criminalizing masturbation? I suspect most readers will conclude the answer is "no" and also that this is likely for the best. But consider the paragraph at the end of Kennedy's opinion explaining that the present case does not concern minors, injury, public conduct, or a variety of other factors. How much of Scalia's list can be addressed using Kennedy's factors?
2. The Supreme Court (with Kennedy writing) later held that a federal prohibition on same-sex marriage violated the due process clause. *United States v. Windsor*, 570 U.S. 744 (2013). "The federal statute is invalid, for no legitimate purpose overcomes the purpose and effect to disparage and to injure those whom the State, by its marriage laws, sought to protect in personhood and dignity." Two years after *Windsor*, the Court further held that state laws prohibiting same-sex marriage were also violations of due process. *Obergefell v. Hodges*, 576 U.S. 644 (2015). "The Constitution promises liberty to all within its reach a liberty that includes certain specific rights that allow persons, within a lawful realm, to define and express their identity." Kennedy's majority grounded its holding in the fundamental importance of marriage: "The nature of marriage is that, through its enduring bond, two persons together can find other freedoms, such as expression, intimacy, and spirituality. This is true for all persons, whatever their sexual orientation."
3. How best to define fundamental rights? There obviously is no historical support for a right to "same-sex marriage" any more than there is a right to "homosexual sodomy." But there is historical support for a right to "marriage" and, post-*Griswold*, a right to private intimate relations of some sort. Kennedy in *Obergefell* points out that the Court did not ask whether there was a right to "interracial marriage" or "inmate marriage" when it struck down prohibitions on those practices but instead whether there was a right to "marriage." So marriage is the relevant unit of analysis. How well does that square with *Glucksberg* concern about broad and vaguely defined rights?

B. Dobbs and the future of the right to decision privacy

Coming out of *Lawrence* and *Windsor* there was a sense that the constitutional right to privacy was on firm ground; that the Court's previous holdings in that area were safe; and that there was room to expand the right to privacy to address new social issues. One could imagine Kennedy firing up a typewriter to address gender-affirming care, for instance.[132] How does the *Dobbs* case below impact your understanding of the future direction of decision privacy? Is *Dobbs* a general reining in of due process jurisprudence, or is it restricted to the abortion space?

Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022)

Justice ALITO delivered the opinion of the Court.

[132] *See, e.g.*, Kyle C. Velte, *Mitigating the "LGBT Disconnect": Title IX's Protection of Transgender Students, Birth Certificate Correction Statutes, and the Transformative Potential of Connecting the Two*, 27 AM. U. J. GENDER SOC. POL'Y & L. 29, 74 (2019) ("It is a short line indeed to connect the Court's holdings regarding identity, dignity, and personal autonomy for LGB people to the identity, dignity, and personal autonomy for transgender people.").

Abortion presents a profound moral issue on which Americans hold sharply conflicting views. Some believe fervently that a human person comes into being at conception and that abortion ends an innocent life. Others feel just as strongly that any regulation of abortion invades a woman's right to control her own body and prevents women from achieving full equality. Still others in a third group think that abortion should be allowed under some but not all circumstances, and those within this group hold a variety of views about the particular restrictions that should be imposed.

For the first 185 years after the adoption of the Constitution, each State was permitted to address this issue in accordance with the views of its citizens. Then, in 1973, this Court decided *Roe v. Wade*. Even though the Constitution makes no mention of abortion, the Court held that it confers a broad right to obtain one. It did not claim that American law or the common law had ever recognized such a right, and its survey of history ranged from the constitutionally irrelevant (*e.g.*, its discussion of abortion in antiquity) to the plainly incorrect (*e.g.*, its assertion that abortion was probably never a crime under the common law). After cataloging a wealth of other information having no bearing on the meaning of the Constitution, the opinion concluded with a numbered set of rules much like those that might be found in a statute enacted by a legislature.

Under this scheme, each trimester of pregnancy was regulated differently, but the most critical line was drawn at roughly the end of the second trimester, which, at the time, corresponded to the point at which a fetus was thought to achieve "viability," *i.e.*, the ability to survive outside the womb. Although the Court acknowledged that States had a legitimate interest in protecting "potential life," it found that this interest could not justify any restriction on pre-viability abortions. The Court did not explain the basis for this line, and even abortion supporters have found it hard to defend *Roe*'s reasoning.

At the time of *Roe*, 30 States still prohibited abortion at all stages. In the years prior to that decision, about a third of the States had liberalized their laws, but *Roe* abruptly ended that political process. It imposed the same highly restrictive regime on the entire Nation, and it effectively struck down the abortion laws of every single State. As Justice Byron White aptly put it in his dissent, the decision represented the "exercise of raw judicial power," and it sparked a national controversy that has embittered our political culture for a half century.

Eventually, in *Planned Parenthood of Southeastern Pa. v. Casey* (1992), the Court revisited *Roe*, but the Members of the Court split three ways. But the three Justices who authored the controlling opinion "call[ed] the contending sides of a national controversy to end their national division" by treating the Court's decision as the final settlement of the question of the constitutional right to abortion.

As has become increasingly apparent in the intervening years, *Casey* did not achieve that goal. Americans continue to hold passionate and widely divergent views on abortion, and state legislatures have acted accordingly. Some have recently enacted laws allowing abortion, with few restrictions, at all stages of pregnancy. Others have tightly restricted abortion beginning well before viability. And in this case, 26 States have expressly asked this Court to overrule *Roe* and *Casey* and allow the States to regulate or prohibit pre-viability abortions.

We hold that *Roe* and *Case*y must be overruled. The Constitution makes no reference to abortion, and no such right is implicitly protected by any constitutional provision, including the one on which the defenders of *Roe* and *Casey* now chiefly rely—the Due Process Clause of the Fourteenth Amendment. That provision has been held to guarantee some rights that are not mentioned in the Constitution, but any such right must be "deeply rooted in this Nation's history and tradition" and "implicit in the concept of ordered liberty." *Washington v.* Glucksberg (1997).

The right to abortion does not fall within this category. Until the latter part of the 20th century, such a right was entirely unknown in American law. Indeed, when the Fourteenth

Amendment was adopted, three quarters of the States made abortion a crime at all stages of pregnancy. The abortion right is also critically different from any other right that this Court has held to fall within the Fourteenth Amendment's protection of "liberty." *Roe*'s defenders characterize the abortion right as similar to the rights recognized in past decisions involving matters such as intimate sexual relations, contraception, and marriage, but abortion is fundamentally different, as both *Roe* and *Casey* acknowledged, because it destroys what those decisions called "fetal life" and what the law now before us describes as an "unborn human being."

The underlying theory on which this argument rests—that the Fourteenth Amendment's Due Process Clause provides substantive, as well as procedural, protection for "liberty"—has long been controversial. But our decisions have held that the Due Process Clause protects two categories of substantive rights.

The first consists of rights guaranteed by the first eight Amendments. Those Amendments originally applied only to the Federal Government, but this Court has held that the Due Process Clause of the Fourteenth Amendment "incorporates" the great majority of those rights and thus makes them equally applicable to the States. The second category—which is the one in question here—comprises a select list of fundamental rights that are not mentioned anywhere in the Constitution.

In deciding whether a right falls into either of these categories, the Court has long asked whether the right is "deeply rooted in [our] history and tradition" and whether it is essential to our Nation's "scheme of ordered liberty." And in conducting this inquiry, we have engaged in a careful analysis of the history of the right at issue.

Historical inquiries of this nature are essential whenever we are asked to recognize a new component of the "liberty" protected by the Due Process Clause because the term "liberty" alone provides little guidance. "Liberty" is a capacious term. As Lincoln once said: "We all declare for Liberty; but in using the same word we do not all mean the same thing."

In interpreting what is meant by the Fourteenth Amendment's reference to "liberty," we must guard against the natural human tendency to confuse what that Amendment protects with our own ardent views about the liberty that Americans should enjoy. That is why the Court has long been "reluctant" to recognize rights that are not mentioned in the Constitution.

Until the latter part of the 20th century, there was no support in American law for a constitutional right to obtain an abortion. Not only was there no support for such a constitutional right until shortly before *Roe*, but abortion had long been a *crime* in every single State. At common law, abortion was criminal in at least some stages of pregnancy and was regarded as unlawful and could have very serious consequences at all stages. American law followed the common law until a wave of statutory restrictions in the 1800s expanded criminal liability for abortions. By the time of the adoption of the Fourteenth Amendment, three-quarters of the States had made abortion a crime at any stage of pregnancy, and the remaining States would soon follow.

*A*lthough a pre-quickening abortion was not itself considered homicide, it does not follow that abortion was *permissible* at common law—much less that abortion was a legal *right*.

Instead of seriously pressing the argument that the abortion right itself has deep roots, supporters of *Roe* and *Casey* contend that the abortion right is an integral part of a broader entrenched right. *Roe* termed this a right to privacy, and *Casey* described it as the freedom to make "intimate and personal choices" that are "central to personal dignity and autonomy." *Casey* elaborated: "At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life."

The Court did not claim that this broadly framed right is absolute, and no such claim would be plausible. While individuals are certainly free *to think* and *to say* what they wish about

"existence," "meaning," the "universe," and "the mystery of human life," they are not always free *to act* in accordance with those thoughts. License to act on the basis of such beliefs may correspond to one of the many understandings of "liberty," but it is certainly not "ordered liberty."

Ordered liberty sets limits and defines the boundary between competing interests. *Roe* and *Casey* each struck a particular balance between the interests of a woman who wants an abortion and the interests of what they termed "potential life." But the people of the various States may evaluate those interests differently. In some States, voters may believe that the abortion right should be even more extensive than the right that *Roe* and *Casey* recognized. Voters in other States may wish to impose tight restrictions based on their belief that abortion destroys an "unborn human being." Miss. Code Ann. § 41–41–191(4)(b). Our Nation's historical understanding of ordered liberty does not prevent the people's elected representatives from deciding how abortion should be regulated.

These attempts to justify abortion through appeals to a broader right to autonomy and to define one's "concept of existence" prove too much criteria, at a high level of generality, could license fundamental rights to illicit drug use, prostitution, and the like. None of these rights has any claim to being deeply rooted in history.

In drawing this critical distinction between the abortion right and other rights, it is not necessary to dispute *Casey*'s claim (which we accept for the sake of argument) that "the specific practices of States at the time of the adoption of the Fourteenth Amendment" do not "mar[k] the outer limits of the substantive sphere of liberty which the Fourteenth Amendment protects." Abortion is nothing new. It has been addressed by lawmakers for centuries, and the fundamental moral question that it poses is ageless.

Defenders of *Roe* and *Casey* do not claim that any new scientific learning calls for a different answer to the underlying moral question, but they do contend that changes in society require the recognition of a constitutional right to obtain an abortion. Without the availability of abortion, they maintain, people will be inhibited from exercising their freedom to choose the types of relationships they desire, and women will be unable to compete with men in the workplace and in other endeavors.

Americans who believe that abortion should be restricted press countervailing arguments about modern developments. They note that attitudes about the pregnancy of unmarried women have changed drastically; that federal and state laws ban discrimination on the basis of pregnancy; that leave for pregnancy and childbirth are now guaranteed by law in many cases; that the costs of medical care associated with pregnancy are covered by insurance or government assistance; that States have increasingly adopted "safe haven" laws, which generally allow women to drop off babies anonymously; and that a woman who puts her newborn up for adoption today has little reason to fear that the baby will not find a suitable home. They also claim that many people now have a new appreciation of fetal life and that when prospective parents who want to have a child view a sonogram, they typically have no doubt that what they see is their daughter or son.

Finally, after all this, the Court turned to precedent. Citing a broad array of cases, the Court found support for a constitutional "right of personal privacy," but it conflated two very different meanings of the term: the right to shield information from disclosure and the right to make and implement important personal decisions without governmental interference. Only the cases involving this second sense of the term could have any possible relevance to the abortion issue, and some of the cases in that category involved personal decisions that were obviously very, very far afield. What remained was a handful of cases having something to do with marriage or procreation. But none of these decisions involved what is distinctive about abortion: its effect on what *Roe* termed "potential life."

Finally, the dissent suggests that our decision calls into question *Griswold*, *Eisenstadt*, *Lawrence*, and *Obergefell*. But we have stated unequivocally that "[n]othing in this opinion should be understood to cast doubt on precedents that do not concern abortion." We have also explained why that is so: rights regarding contraception and same-sex relationships are inherently different from the right to abortion because the latter (as we have stressed) uniquely involves what *Roe* and *Casey* termed "potential life." Therefore, a right to abortion cannot be justified by a purported analogy to the rights recognized in those other cases or by "appeals to a broader right to autonomy." It is hard to see how we could be clearer.

We end this opinion where we began. Abortion presents a profound moral question. The Constitution does not prohibit the citizens of each State from regulating or prohibiting abortion. *Roe* and *Casey* arrogated that authority. We now overrule those decisions and return that authority to the people and their elected representatives.

Justice THOMAS, concurring.

I join the opinion of the Court because it correctly holds that there is no constitutional right to abortion. Respondents invoke one source for that right: the Fourteenth Amendment's guarantee that no State shall "deprive any person of life, liberty, or property without due process of law."

As I have previously explained, "substantive due process" is an oxymoron that "lack[s] any basis in the Constitution." "The notion that a constitutional provision that guarantees only 'process' before a person is deprived of life, liberty, or property could define the substance of those rights strains credulity for even the most casual user of words." The resolution of this case is thus straightforward. Because the Due Process Clause does not secure *any* substantive rights, it does not secure a right to abortion.

The Court today declines to disturb substantive due process jurisprudence generally or the doctrine's application in other, specific contexts. Cases like *Griswold v. Connecticut* (1965) (right of married persons to obtain contraceptives); *Lawrence v. Texas* (2003) (right to engage in private, consensual sexual acts); and *Obergefell v. Hodges* (2015) (right to same-sex marriage), are not at issue. The Court's abortion cases are unique, and no party has asked us to decide "whether our entire Fourteenth Amendment jurisprudence must be preserved or revised." Thus, I agree that "[n]othing in [the Court's] opinion should be understood to cast doubt on precedents that do not concern abortion."

For that reason, in future cases, we should reconsider all of this Court's substantive due process precedents, including *Griswold*, *Lawrence*, and *Obergefell*. Because any substantive due process decision is "demonstrably erroneous."

Justice KAVANAUGH, concurring.

On the question of abortion, the Constitution is therefore neither pro-life nor pro-choice. The Constitution is neutral and leaves the issue for the people and their elected representatives to resolve through the democratic process in the States or Congress—like the numerous other difficult questions of American social and economic policy that the Constitution does not address.

Because the Constitution is neutral on the issue of abortion, this Court also must be scrupulously neutral. The nine unelected Members of this Court do not possess the constitutional authority to override the democratic process and to decree either a pro-life or a pro-choice abortion policy for all 330 million people in the United States.

To be clear, then, the Court's decision today *does not outlaw* abortion throughout the United States. On the contrary, the Court's decision properly leaves the question of abortion for the people and their elected representatives in the democratic process.

Chief Justice ROBERTS, concurring in the judgment.

In short, the viability rule was created outside the ordinary course of litigation, is and always has been completely unreasoned, and fails to take account of state interests since recognized as legitimate. It is indeed "telling that other countries almost uniformly eschew" a viability line. Only a handful of countries, among them China and North Korea, permit elective abortions after twenty weeks; the rest have coalesced around a 12–week line. The Court rightly rejects the arbitrary viability rule today.

None of this, however, requires that we also take the dramatic step of altogether eliminating the abortion right first recognized in *Roe*. Mississippi itself previously argued as much to this Court in this litigation.

Here, there is a clear path to deciding this case correctly without overruling *Roe* all the way down to the studs: recognize that the viability line must be discarded, as the majority rightly does, and leave for another day whether to reject any right to an abortion at all.

The Court's decision to overrule *Roe* and *Casey* is a serious jolt to the legal system—regardless of how you view those cases. A narrower decision rejecting the misguided viability line would be markedly less unsettling, and nothing more is needed to decide this case.

Justice BREYER, Justice SOTOMAYOR, and Justice KAGAN, dissenting.

For half a century, *Roe v. Wade* (1973) and *Planned Parenthood of Southeastern Pa. v. Casey* (1992) have protected the liberty and equality of women. *Roe* held, and *Casey* reaffirmed, that the Constitution safeguards a woman's right to decide for herself whether to bear a child. *Roe* held, and *Casey* reaffirmed, that in the first stages of pregnancy, the government could not make that choice for women. The government could not control a woman's body or the course of a woman's life: It could not determine what the woman's future would be. Respecting a woman as an autonomous being, and granting her full equality, meant giving her substantial choice over this most personal and most consequential of all life decisions.

Roe and *Casey* well understood the difficulty and divisiveness of the abortion issue. The Court knew that Americans hold profoundly different views about the "moral[ity]" of "terminating a pregnancy, even in its earliest stage." And the Court recognized that "the State has legitimate interests from the outset of the pregnancy in protecting" the "life of the fetus that may become a child. So the Court struck a balance, as it often does when values and goals compete. It held that the State could prohibit abortions after fetal viability, so long as the ban contained exceptions to safeguard a woman's life or health. It held that even before viability, the State could regulate the abortion procedure in multiple and meaningful ways. But until the viability line was crossed, the Court held, a State could not impose a "substantial obstacle" on a woman's "right to elect the procedure" as she (not the government) thought proper, in light of all the circumstances and complexities of her own life.

The majority makes this change based on a single question: Did the reproductive right recognized in *Roe* and *Casey* exist in "1868, the year when the Fourteenth Amendment was ratified"? The majority says (and with this much we agree) that the answer to this question is no: In 1868, there was no nationwide right to end a pregnancy, and no thought that the Fourteenth Amendment provided one.

Second—and embarrassingly for the majority—early law in fact does provide some support for abortion rights. Common-law authorities did not treat abortion as a crime before "quickening"—the point when the fetus moved in the womb. And early American law followed the common-law rule. So the criminal law of that early time might be taken as roughly consonant with *Roe*'s and *Casey*'s different treatment of early and late abortions.

The majority's core legal postulate, then, is that we in the 21st century must read the Fourteenth Amendment just as its ratifiers did. And that is indeed what the majority

emphasizes over and over again. If the ratifiers did not understand something as central to freedom, then neither can we. Or said more particularly: If those people did not understand reproductive rights as part of the guarantee of liberty conferred in the Fourteenth Amendment, then those rights do not exist.

As an initial matter, note a mistake in the just preceding sentence. We referred there to the "people" who ratified the Fourteenth Amendment: What rights did those "people" have in their heads at the time? But, of course, "people" did not ratify the Fourteenth Amendment. Men did. So it is perhaps not so surprising that the ratifiers were not perfectly attuned to the importance of reproductive rights for women's liberty, or for their capacity to participate as equal members of our Nation. Indeed, the ratifiers—both in 1868 and when the original Constitution was approved in 1788—did not understand women as full members of the community embraced by the phrase "We the People." In 1868, the first wave of American feminists were explicitly told—of course by men—that it was not their time to seek constitutional protections. (Women would not get even the vote for another half-century.) To be sure, most women in 1868 also had a foreshortened view of their rights: If most men could not then imagine giving women control over their bodies, most women could not imagine having that kind of autonomy. But that takes away nothing from the core point. Those responsible for the original Constitution, including the Fourteenth Amendment, did not perceive women as equals, and did not recognize women's rights. When the majority says that we must read our foundational charter as viewed at the time of ratification (except that we may also check it against the Dark Ages), it consigns women to second-class citizenship.

Casey itself understood this point, as will become clear. It recollected with dismay a decision this Court issued just five years after the Fourteenth Amendment's ratification, approving a State's decision to deny a law license to a woman and suggesting as well that a woman had no legal status apart from her husband. But times had changed. A woman's place in society had changed, and constitutional law had changed along with it. The relegation of women to inferior status in either the public sphere or the family was "no longer consistent with our understanding" of the Constitution. Now, "[t]he Constitution protects all individuals, male or female," from "the abuse of governmental power" or "unjustified state interference."

So how is it that, as *Casey* said, our Constitution, read now, grants rights to women, though it did not in 1868? How is it that our Constitution subjects discrimination against them to heightened judicial scrutiny? How is it that our Constitution, through the Fourteenth Amendment's liberty clause, guarantees access to contraception (also not legally protected in 1868) so that women can decide for themselves whether and when to bear a child? How is it that until today, that same constitutional clause protected a woman's right, in the event contraception failed, to end a pregnancy in its earlier stages?

The answer is that this Court has rejected the majority's pinched view of how to read our Constitution. "The Founders," we recently wrote, "knew they were writing a document designed to apply to ever-changing circumstances over centuries." Or in the words of the great Chief Justice John Marshall, our Constitution is "intended to endure for ages to come," and must adapt itself to a future "seen dimly," if at all. That is indeed why our Constitution is written as it is. The Framers (both in 1788 and 1868) understood that the world changes. So they did not define rights by reference to the specific practices existing at the time. Instead, the Framers defined rights in general terms, to permit future evolution in their scope and meaning. And over the course of our history, this Court has taken up the Framers' invitation. It has kept true to the Framers' principles by applying them in new ways, responsive to new societal understandings and conditions.

And liberty may require it, this Court has repeatedly said, even when those living in 1868 would not have recognized the claim—because they would not have seen the person making it as a full-fledged member of the community. Throughout our history, the sphere of protected liberty has expanded, bringing in individuals formerly excluded. In that way, the

constitutional values of liberty and equality go hand in hand; they do not inhabit the hermetically sealed containers the majority portrays. So before *Roe* and *Casey*, the Court expanded in successive cases those who could claim the right to marry—though their relationships would have been outside the law's protection in the mid-19th century. And after *Roe* and *Casey*, of course, the Court continued in that vein. With a critical stop to hold that the Fourteenth Amendment protected same-sex intimacy, the Court resolved that the Amendment also conferred on same-sex couples the right to marry. In considering that question, the Court held, "[h]istory and tradition," especially as reflected in the course of our precedent, "guide and discipline [the] inquiry." But the sentiments of 1868 alone do not and cannot "rule the present."

Notes

1. The majority in *Dobbs* is trying mightily to separate the issue of abortion from other due process cases. Abortion concerns potential life; same-sex marriage and contraception do not. Are they persuasive in their attempt to draw this distinction?
2. Unique to the abortion context on a practical level is the multi-decade-long political campaign to make the Court overturn *Roe*. Though decisions protecting interracial marriage and same-sex marriage were highly controversial when they were decided, their salience diminished sharply over time. A search of news articles finds little mention of protests against same-sex marriage in the United States since 2016 even though the issue was vigorously debated prior to the Court's decision. Does this inform our understanding of due process and fundamental rights?
3. From *Glucksberg* to *Lawrence* to *Dobbs* we have had shifting conceptions of how privacy rights should be defined. Are the rights very narrowly construed, construed to reflect broad underlying principles, or somewhere in between? How much does *Dobbs* itself shift your understanding of how to define rights?
4. The dissent gives full-throated endorsement of a form of living constitutionalism. In their view, the polity of the 1860s was fundamentally wrong about key issues, including basic questions of who should count as a member of the polity. In the dissenters' view, we will discover that we must protect new rights if we take the conception of liberty that once applied only to certain people and instead apply it to all people. How comfortable are you with this view? Does it give too much power to courts to remove issues from the democratic debate? Or is it a necessary insight given the limited political power of groups that were previously and wrongfully[133] excluded from the political debate?

C. The right to information privacy

Developing parallel to the prior decisional privacy cases is a line of cases addressing the potential constitutional right to information privacy. The possibility of this right was first clearly articulated in *Whalen v. Roe* (1977).

1) Foundations

Whalen v. Roe, 429 U.S. 589 (1977)

Mr. Justice STEVENS delivered the opinion of the Court.

The constitutional question presented is whether the State of New York may record, in a centralized computer file, the names and addresses of all persons who have obtained,

[133] There is obviously a value judgement here about who is wrongfully excluded. I suspect few law students will argue against women's suffrage, but not all issues have that level of consensus. That is part of the challenge here. Think back to *Lawrence* and whether moral disapproval can ever be a basis for discriminating against a group.

pursuant to a doctor's prescription, certain drugs for which there is both a lawful and an unlawful market.

The District Court enjoined enforcement of the portions of the New York State Controlled Substances Act of 1972 which require such recording on the ground that they violate appellees' constitutionally protected rights of privacy. We noted probable jurisdiction of the appeal by the Commissioner of Health and now reverse.

Many drugs have both legitimate and illegitimate uses. In response to a concern that such drugs were being diverted into unlawful channels, in 1970 the New York Legislature created a special commission to evaluate the State's drug-control laws. The commission found the existing laws deficient in several respects. There was no effective way to prevent the use of stolen or revised prescriptions, to prevent unscrupulous pharmacists from repeatedly refilling prescriptions, to prevent users from obtaining prescriptions from more than one doctor, or to prevent doctors from over-prescribing, either by authorizing an excessive amount in one prescription or by giving one patient multiple prescriptions. In drafting new legislation to correct such defects, the commission consulted with enforcement officials in California and Illinois where central reporting systems were being used effectively.

The new New York statute classified potentially harmful drugs in five schedules. Drugs, such as heroin, which are highly abused and have no recognized medical use, are in Schedule I; they cannot be prescribed. Schedules II through V include drugs which have a progressively lower potential for abuse but also have a recognized medical use. Our concern is limited to Schedule II which includes the most dangerous of the legitimate drugs.[8]

With an exception for emergencies, the Act requires that all prescriptions for Schedule II drugs be prepared by the physician in triplicate on an official form. The completed form identifies the prescribing physician; the dispensing pharmacy; the drug and dosage; and the name, address, and age of the patient. One copy of the form is retained by the physician, the second by the pharmacist, and the third is forwarded to the New York State Department of Health in Albany. A prescription made on an official form may not exceed a 30-day supply, and may not be refilled.

The District Court found that about 100,000 Schedule II prescription forms are delivered to a receiving room at the Department of Health in Albany each month. They are sorted, coded, and logged and then taken to another room where the data on the forms is recorded on magnetic tapes for processing by a computer. Thereafter, the forms are returned to the receiving room to be retained in a vault for a five-year period and then destroyed as required by the statute. The receiving room is surrounded by a locked wire fence and protected by an alarm system. The computer tapes containing the prescription data are kept in a locked cabinet. When the tapes are used, the computer is run “off-line,” which means that no terminal outside of the computer room can read or record any information. Public disclosure of the identity of patients is expressly prohibited by the statute and by a Department of Health regulation. Willful violation of these prohibitions is a crime punishable by up to one year in prison and a $2,000 fine. At the time of trial there were 17 Department of Health employees with access to the files; in addition, there were 24 investigators with authority to investigate cases of overdispensing which might be identified by the computer. Twenty months after the effective date of the Act, the computerized data had only been used in two investigations involving alleged overuse by specific patients.

A few days before the Act became effective, this litigation was commenced by a group of patients regularly receiving prescriptions for Schedule II drugs, by doctors who prescribe such

---

[8] These include opium and opium derivatives, cocaine, methadone, amphetamines, and methaqualone. These drugs have accepted uses in the amelioration of pain and in the treatment of epilepsy, narcolepsy, hyperkinesia, schizo-affective disorders, and migraine headaches.

drugs, and by two associations of physicians. After various preliminary proceedings, a three-judge District Court conducted a one-day trial. Appellees offered evidence tending to prove that persons in need of treatment with Schedule II drugs will from time to time decline such treatment because of their fear that the misuse of the computerized data will cause them to be stigmatized as "drug addicts."[16]

The District Court found that the State had been unable to demonstrate the necessity for the patient-identification requirement on the basis of its experience during the first 20 months of administration of the new statute.

State legislation which has some effect on individual liberty or privacy may not be held unconstitutional simply because a court finds it unnecessary, in whole or in part. For we have frequently recognized that individual States have broad latitude in experimenting with possible solutions to problems of vital local concern.

The New York statute challenged in this case represents a considered attempt to deal with such a problem. It is manifestly the product of an orderly and rational legislative decision. It was recommended by a specially appointed commission which held extensive hearings on the proposed legislation, and drew on experience with similar programs in other States. There surely was nothing unreasonable in the assumption that the patient-identification requirement might aid in the enforcement of laws designed to minimize the misuse of dangerous drugs. For the requirement could reasonably be expected to have a deterrent effect on potential violators as well as to aid in the detection or investigation of specific instances of apparent abuse. At the very least, it would seem clear that the State's vital interest in controlling the distribution of dangerous drugs would support a decision to experiment with new techniques for control. For if an experiment fails if in this case experience teaches that the patient-identification requirement results in the foolish expenditure of funds to acquire a mountain of useless information the legislative process remains available to terminate the unwise experiment. It follows that the legislature's enactment of the patient-identification requirement was a reasonable exercise of New York's broad police powers. The District Court's finding that the necessity for the requirement had not been proved is not, therefore, a sufficient reason for holding the statutory requirement unconstitutional.

Appellees contend that the statute invades a constitutionally protected "zone of privacy." The cases sometimes characterized as protecting "privacy" have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions. Appellees argue that both of these interests are impaired by this statute. The mere existence in readily available form of the information about patients' use of Schedule II drugs creates a genuine concern that the information will become publicly known and that it will adversely affect their reputations. This concern makes some patients reluctant to use, and some doctors reluctant to prescribe, such drugs even when their use is medically indicated. It follows, they argue, that the making of decisions about matters vital to the care of their health is

[16] Two parents testified that they were concerned that their children would be stigmatized by the State's central filing system. One child had been taken off his Schedule II medication because of this concern. Three adult patients testified that they feared disclosure of their names would result from central filing of patient identifications. One of them now obtains his drugs in another State. The other two continue to receive Schedule II prescriptions in New York, but continue to fear disclosure and stigmatization. Four physicians testified that the prescription system entrenches on patients' privacy, and that each had observed a reaction of shock, fear, and concern on the part of their patients whom they had informed of the plan. One doctor refuses to prescribe Schedule II drugs for his patients. On the other hand, over 100,000 patients per month have been receiving Schedule II drug prescriptions without their objections, if any, to central filing having come to the attention of the District Court. The record shows that the provisions of the Act were brought to the attention of the section on psychiatry of the New York State Medical Society (App. 166a), but that body apparently declined to support this suit.

inevitably affected by the statute. Thus, the statute threatens to impair both their interest in the nondisclosure of private information and also their interest in making important decisions independently.

We are persuaded, however, that the New York program does not, on its face, pose a sufficiently grievous threat to either interest to establish a constitutional violation.

Public disclosure of patient information can come about in three ways. Health Department employees may violate the statute by failing, either deliberately or negligently, to maintain proper security. A patient or a doctor may be accused of a violation and the stored data may be offered in evidence in a judicial proceeding. Or, thirdly, a doctor, a pharmacist, or the patient may voluntarily reveal information on a prescription form.

The third possibility existed under the prior law and is entirely unrelated to the existence of the computerized data bank. Neither of the other two possibilities provides a proper ground for attacking the statute as invalid on its face. There is no support in the record, or in the experience of the two States that New York has emulated, for an assumption that the security provisions of the statute will be administered improperly. And the remote possibility that judicial supervision of the evidentiary use of particular items of stored information will provide inadequate protection against unwarranted disclosures is surely not a sufficient reason for invalidating the entire patient-identification program.

Even without public disclosure, it is, of course, true that private information must be disclosed to the authorized employees of the New York Department of Health. Such disclosures, however, are not significantly different from those that were required under the prior law. Nor are they meaningfully distinguishable from a host of other unpleasant invasions of privacy that are associated with many facets of health care. Unquestionably, some individuals' concern for their own privacy may lead them to avoid or to postpone needed medical attention. Nevertheless, disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient.[29] Requiring such disclosures to representatives of the State having responsibility for the health of the community, does not automatically amount to an impermissible invasion of privacy.

Appellees also argue, however, that even if unwarranted disclosures do not actually occur, the knowledge that the information is readily available in a computerized file creates a genuine concern that causes some persons to decline needed medication. The record supports the conclusion that some use of Schedule II drugs has been discouraged by that concern; it also is clear, however, that about 100,000 prescriptions for such drugs were being filled each month prior to the entry of the District Court's injunction. Clearly, therefore, the statute did not deprive the public of access to the drugs.

Nor can it be said that any individual has been deprived of the right to decide independently, with the advice of his physician, to acquire and to use needed medication. Although the State no doubt could prohibit entirely the use of particular Schedule II drugs, it has not done so. This case is therefore unlike those in which the Court held that a total prohibition of certain conduct was an impermissible deprivation of liberty. Nor does the State require access to these drugs to be conditioned on the consent of any state official or other third party. Within dosage limits which appellees do not challenge, the decision to prescribe, or to use, is left entirely to the physician and the patient.

We hold that neither the immediate nor the threatened impact of the patient-identification requirements in the New York State Controlled Substances Act of 1972 on either

---

[29] Familiar examples are statutory reporting requirements relating to venereal disease, child abuse, injuries caused by deadly weapons, and certifications of fetal death.

the reputation or the independence of patients for whom Schedule II drugs are medically indicated is sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment.

A final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.

Mr. Justice BRENNAN, concurring.

I write only to express my understanding of the opinion of the Court, which I join.

The New York statute under attack requires doctors to disclose to the State information about prescriptions for certain drugs with a high potential for abuse, and provides for the storage of that information in a central computer file. The Court recognizes that an individual's "interest in avoiding disclosure of personal matters" is an aspect of the right of privacy, but holds that in this case, any such interest has not been seriously enough invaded by the State to require a showing that its program was indispensable to the State's effort to control drug abuse.

The information disclosed by the physician under this program is made available only to a small number of public health officials with a legitimate interest in the information. As the record makes clear, New York has long required doctors to make this information available to its officials on request, and that practice is not challenged here. Such limited reporting requirements in the medical field are familiar and are not generally regarded as an invasion of privacy. Broad dissemination by state officials of such information, however, would clearly implicate constitutionally protected privacy rights, and would presumably be justified only by compelling state interests.

What is more troubling about this scheme, however, is the central computer storage of the data thus collected. Obviously, as the State argues, collection and storage of data by the State that is in itself legitimate is not rendered unconstitutional simply because new technology makes the State's operations more efficient. However, as the example of the Fourth Amendment shows the Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.

In this case, as the Court's opinion makes clear, the State's carefully designed program includes numerous safeguards intended to forestall the danger of indiscriminate disclosure. Given this serious and, so far as the record shows, successful effort to prevent abuse and limit access to the personal information at issue, I cannot say that the statute's provisions for computer storage, on their face, amount to a deprivation of constitutionally protected privacy interests, any more than the more traditional reporting provisions.

In the absence of such a deprivation, the State was not required to prove that the challenged statute is absolutely necessary to its attempt to control drug abuse. Of course, a statute that did effect such a deprivation would only be consistent with the Constitution if it were necessary to promote a compelling state interest.

Notes

1. Much in *Whalen* should be familiar to any student of health privacy. There is no federal doctor–patient evidentiary privilege and, in states where it does exist, such a privilege is limited. More generally, a physician's duty of confidentiality to patients is circumscribed by a variety of exceptions, including ones mandated by the protection of the patient, those close to the patient, and society at large. New in *Whalen* is this idea of a centralized database. So not only does a doctor know what they prescribed, so too does a state agency. Should this distinction matter? The doctor already has to inform a pharmacist, a pharmacy technician, a health insurance company, a billing company, and who knows how many other actors about what they have prescribed. Does disclosure to the state, in addition to all these other actors, make a difference? Possibly yes. The state has a different relationship to the patient/citizen than does any of those other actors. Only the state is in a position to incarcerate.
2. Key in *Whalen* is the idea of safeguards. Safeguards also become important in special needs cases under the Fourth Amendment. In fact, there may be little difference between a constitutional right to information privacy case based upon an act of information acquisition and a Fourth Amendment case based upon the same. Given the uncertainty surrounding the constitutional right to information privacy, plaintiffs appear to more frequently raise the comparatively straightforward Fourth Amendment issue, though sometimes both challenges are made.

Whalen held, in effect, that if a constitutional right to information privacy exists, it was not violated by the New York statute. This is far from a ringing endorsement of the right. The Supreme Court has said remarkably little about this cause of action in subsequent decades. Its most notable statement was in *NASA v. Nelson*.

National Aeronautics and Space Administration v. Nelson, 562 U.S. 134 (2011)

Justice ALITO delivered the opinion of the Court.

In two cases decided more than 30 years ago, this Court referred broadly to a constitutional privacy "interest in avoiding disclosure of personal matters." *Whalen v. Roe* (1977); *Nixon v. Administrator of General Services* (1977). Respondents in this case, federal contract employees at a Government laboratory, claim that two parts of a standard employment background investigation violate their rights under *Whalen* and *Nixon*. Respondents challenge a section of a form questionnaire that asks employees about treatment or counseling for recent illegal-drug use. They also object to certain open-ended questions on a form sent to employees' designated references.

We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*. We hold, however, that the challenged portions of the Government's background check do not violate this right in the present case. The Government's interests as employer and proprietor in managing its internal operations, combined with the protections against public dissemination provided by the Privacy Act of 1974, satisfy any "interest in avoiding disclosure" that may "arguably ha[ve] its roots in the Constitution."

The National Aeronautics and Space Administration (NASA) is an independent federal agency charged with planning and conducting the Government's "space activities." NASA's work force numbers in the tens of thousands of employees. While many of these workers are federal civil servants, a substantial majority are employed directly by Government contractors.

Contract employees play an important role in NASA's mission, and their duties are functionally equivalent to those performed by civil servants.

One NASA facility, the Jet Propulsion Laboratory (JPL) in Pasadena, California, is staffed exclusively by contract employees. NASA owns JPL, but the California Institute of Technology (Cal Tech) operates the facility under a Government contract. JPL is the lead NASA center for deep-space robotics and communications.

Twenty-eight JPL employees are respondents here. Many of them have worked at the lab for decades, and none has ever been the subject of a Government background investigation. At the time when respondents were hired, background checks were standard only for federal civil servants. In some instances, individual contracts required background checks for the employees of federal contractors, but no blanket policy was in place.

The Government has recently taken steps to eliminate this two-track approach to background investigations. In 2004, a recommendation by the 9/11 Commission prompted the President to order new, uniform identification standards for "[f]ederal employees," including "contractor employees." The Department of Commerce implemented this directive by mandating that contract employees with long-term access to federal facilities complete a standard background check, typically the National Agency Check with Inquiries (NACI). JPL management informed employees that anyone failing to complete the NACI process by October 2007 would be denied access to JPL and would face termination by Cal Tech.

The NACI process has long been the standard background investigation for prospective civil servants. The process begins when the applicant or employee fills out a form questionnaire. Employees who work in "non-sensitive" positions (as all respondents here do) complete Standard Form 85 (SF–85).

Most of the questions on SF–85 seek basic biographical information: name, address, prior residences, education, employment history, and personal and professional references. The form also asks about citizenship, selective-service registration, and military service. The last question asks whether the employee has "used, possessed, supplied, or manufactured illegal drugs" in the last year. If the answer is yes, the employee must provide details, including information about "any treatment or counseling received." A "truthful response," the form notes, cannot be used as evidence against the employee in a criminal proceeding. The employee must certify that all responses on the form are true and must sign a release authorizing the Government to obtain personal information from schools, employers, and others during its investigation.

Once a completed SF–85 is on file, the "agency check" and "inquiries" begin. The Government runs the information provided by the employee through FBI and other federal-agency databases. It also sends out form questionnaires to the former employers, schools, landlords, and references listed on SF–85. The particular form at issue in this case—the Investigative Request for Personal Information, Form 42—goes to the employee's former landlords and references.

Form 42 is a two-page document that takes about five minutes to complete. It explains to the reference that "[y]our name has been provided by" a particular employee or applicant to help the Government determine that person's "suitability for employment or a security clearance." After several preliminary questions about the extent of the reference's associations with the employee, the form asks if the reference has "any reason to question" the employee's "honesty or trustworthiness." It also asks if the reference knows of any "adverse information" concerning the employee's "violations of the law," "financial integrity," "abuse of alcohol and/or drugs," "mental or emotional stability," "general behavior or conduct," or "other matters." If "yes" is checked for any of these categories, the form calls for an explanation in the space below. That space is also available for providing "additional information" ("derogatory" or "positive") that may bear on "suitability for government employment or a security clearance."

All responses to SF–85 and Form 42 are subject to the protections of the Privacy Act. The Act authorizes the Government to keep records pertaining to an individual only when they are "relevant and necessary" to an end "required to be accomplished" by law. Individuals are permitted to access their records and request amendments to them. Subject to certain exceptions, the Government may not disclose records pertaining to an individual without that individual's written consent.

[R]espondents contend that portions of SF–85 and Form 42 violate their "right to informational privacy." This Court considered a similar claim in *Whalen,* which concerned New York's practice of collecting "the names and addresses of all persons" prescribed dangerous drugs with both "legitimate and illegitimate uses." In discussing that claim, the Court said that "[t]he cases sometimes characterized as protecting 'privacy'" actually involved "at least two different kinds of interests": one, an "interest in avoiding disclosure of personal matters"; the other, an interest in "making certain kinds of important decisions" free from government interference.

Whalen acknowledged that the disclosure of "private information" to the State was an "unpleasant invasio[n] of privacy," but the Court pointed out that the New York statute contained "security provisions" that protected against "[p]ublic disclosure" of patients' information. This sort of "statutory or regulatory duty to avoid unwarranted disclosures" of "accumulated private data" was sufficient, in the Court's view, to protect a privacy interest that "arguably ha[d] its roots in the Constitution." The Court thus concluded that the statute did not violate "any right or liberty protected by the Fourteenth Amendment."

Four months later, the Court referred again to a constitutional "interest in avoiding disclosure." *Nixon*. Former President Nixon brought a challenge to the Presidential Recordings and Materials Preservation Act, a statute that required him to turn over his Presidential papers and tape recordings for archival review and screening. In a section of the opinion entitled "Privacy," the Court addressed a combination of claims that the review required by this Act violated the former President's "Fourth and Fifth Amendmen[t]" rights. The Court rejected those challenges after concluding that the Act at issue, like the statute in *Whalen,* contained protections against "undue dissemination of private materials." Indeed, the Court observed that the former President's claim was "weaker" than the one "found wanting . . . [in] *Whalen,*" as the Government was required to return immediately all "purely private papers and recordings" identified by the archivists. Citing Fourth Amendment precedent, the Court also stated that the public interest in preserving Presidential papers outweighed any "legitimate expectation of privacy" that the former President may have enjoyed.

The Court announced the decision in *Nixon* in the waning days of October Term 1976. Since then, the Court has said little else on the subject of an "individual interest in avoiding disclosure of personal matters."

As was our approach in *Whalen,* we will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance. We hold, however, that, whatever the scope of this interest, it does not prevent the Government from asking reasonable questions of the sort included on SF–85 and Form 42 in an employment background investigation that is subject to the Privacy Act's safeguards against public disclosure.

As an initial matter, judicial review of the Government's challenged inquiries must take into account the context in which they arise. When the Government asks respondents and their references to fill out SF–85 and Form 42, it does not exercise its sovereign power "to regulate or license." *Cafeteria & Restaurant Workers v. McElroy (*1961). Rather, the Government conducts the challenged background checks in its capacity "as proprietor" and manager of its "internal operation." Time and again our cases have recognized that the Government has a much freer hand in dealing "with citizen employees than it does when it brings its sovereign

power to bear on citizens at large." This distinction is grounded on the "common-sense realization" that if every "employment decision became a constitutional matter," the Government could not function.

An assessment of the constitutionality of the challenged portions of SF–85 and Form 42 must account for this distinction. The questions challenged by respondents are part of a standard employment background check of the sort used by millions of private employers. The Government itself has been conducting employment investigations since the earliest days of the Republic. Since 1871, the President has enjoyed statutory authority to "ascertain the fitness of applicants" for the civil service "as to age, health, character, knowledge and ability for the employment sought," and that Act appears to have been regarded as a codification of established practice. Standard background investigations similar to those at issue here became mandatory for all candidates for the federal civil service in 1953.

Respondents argue that, because they are contract employees and not civil servants, the Government's broad authority in managing its affairs should apply with diminished force. But the Government's interest as "proprietor" in managing its operations, does not turn on such formalities. The record shows that, as a "practical matter," there are no "[r]elevant distinctions" between the duties performed by NASA's civil-service work force and its contractor work force. The two classes of employees perform "functionally equivalent duties," and the extent of employees' "access to NASA . . . facilities" turns not on formal status but on the nature of "the jobs they perform."

With these interests in view, we conclude that the challenged portions of both SF–85 and Form 42 consist of reasonable, employment-related inquiries that further the Government's interests in managing its internal operations. As to SF–85, the only part of the form challenged here is its request for information about "any treatment or counseling received" for illegal-drug use within the previous year. The "treatment or counseling" question, however, must be considered in context. It is a followup to SF–85's inquiry into whether the employee has "used, possessed, supplied, or manufactured illegal drugs" during the past year. The Government has good reason to ask employees about their recent illegal-drug use. Like any employer, the Government is entitled to have its projects staffed by reliable, law-abiding persons who will "efficiently and effectively" discharge their duties.

In context, the followup question on "treatment or counseling" for recent illegal-drug use is also a reasonable, employment-related inquiry. The Government, recognizing that illegal-drug use is both a criminal and a medical issue, seeks to separate out those illegal-drug users who are taking steps to address and overcome their problems.

We reject the argument that the Government, when it requests job-related personal information in an employment background check, has a constitutional burden to demonstrate that its questions are "necessary" or the least restrictive means of furthering its interests. So exacting a standard runs directly contrary to *Whalen*.

The Court of Appeals also held that the broad, "open-ended questions" on Form 42 likely violate respondents' informational-privacy rights. Form 42 asks applicants' designated references and landlords for "information" bearing on "suitability for government employment or a security clearance." In a series of questions, the Government asks if the reference has any "adverse information" about the applicant's "honesty or trustworthiness," "violations of the law," "financial integrity," "abuse of alcohol and/or drugs," "mental or emotional stability," "general behavior or conduct," or "other matters."

These open-ended inquiries, like the drug-treatment question on SF–85, are reasonably aimed at identifying capable employees who will faithfully conduct the Government's business. The reasonableness of such open-ended questions is illustrated by their pervasiveness in the public and private sectors. Form 42 alone is sent out by the Government over 1.8 million times

annually. In addition, the use of open-ended questions in employment background checks appears to be equally commonplace in the private sector.

Not only are SF–85 and Form 42 reasonable in light of the Government interests at stake, they are also subject to substantial protections against disclosure to the public. Both *Whalen* and *Nixon* recognized that government "accumulation" of "personal information" for "public purposes" may pose a threat to privacy. But both decisions also stated that a "statutory or regulatory duty to avoid unwarranted disclosures" generally allays these privacy concerns.

Respondents in this case, like the patients in *Whalen* and former President Nixon, attack only the Government's *collection* of information on SF–85 and Form 42. And here, no less than in *Whalen* and *Nixon,* the information collected is shielded by statute from "unwarranted disclosur[e]." The Privacy Act, which covers all information collected during the background-check process, allows the Government to maintain records "about an individual" only to the extent the records are "relevant and necessary to accomplish" a purpose authorized by law. The Act requires written consent before the Government may disclose records pertaining to any individual. And the Act imposes criminal liability for willful violations of its nondisclosure obligations.

Notwithstanding these safeguards, respondents argue that statutory exceptions to the Privacy Act's disclosure bar leave its protections too porous to supply a meaningful check against "unwarranted disclosures." Respondents point in particular to what they describe as a "broad" exception for "routine use[s]," defined as uses that are "compatible with the purpose for which the record was collected." §§ 552a(b)(3), (a)(7).

Nor does the substance of the "routine use" exception relied on by respondents create any undue risk of public dissemination. None of the authorized "routine use[s]" of respondents' background-check information allows for release to the public. Rather, the established "routine use[s]" consist of limited, reasonable steps designed to complete the background-check process in an efficient and orderly manner. The "remote possibility" of public disclosure created by these narrow "routine use[s]" does not undermine the Privacy Act's substantial protections.

Citing past violations of the Privacy Act, respondents note that it is possible that their personal information could be disclosed as a result of a similar breach. But data breaches are a possibility any time the Government stores information. As the Court recognized in *Whalen,* the mere possibility that security measures will fail provides no "proper ground" for a broad-based attack on government information-collection practices.

In light of the protection provided by the Privacy Act's nondisclosure requirement, and because the challenged portions of the forms consist of reasonable inquiries in an employment background check, we conclude that the Government's inquiries do not violate a constitutional right to informational privacy.

Justice SCALIA, with whom Justice THOMAS joins, concurring in the judgment.

I agree with the Court, of course, that background checks of employees of Government contractors do not offend the Constitution. But rather than reach this conclusion on the basis of the never-explained assumption that the Constitution requires courts to "balance" the Government's interests in data collection against its contractor employees' interest in privacy, I reach it on simpler grounds. Like many other desirable things not included in the Constitution, "informational privacy" seems like a good idea . . . . But it is up to the People to enact those laws, to shape them, and, when they think it appropriate, to repeal them. A federal constitutional right to "informational privacy" does not exist.

Before addressing the constitutional issues, however, I must observe a remarkable and telling fact about this case, unique in my tenure on this Court: Respondents' brief, in arguing

that the Federal Government violated the Constitution, does not once identify which provision of the Constitution that might be.

To tell the truth, I found this approach refreshingly honest. One who asks us to invent a constitutional right out of whole cloth should spare himself and us the pretense of tying it to some words of the Constitution. Regrettably, this Lincolnesque honesty evaporated at oral argument, when counsel asserted, apparently for the first time in this litigation, that the right to informational privacy emerged from the Due Process Clause of the Fifth Amendment. That counsel invoked the infinitely plastic concept of "substantive" due process does not make this constitutional theory any less invented.

The absurdity of respondents' position in this case should not, however, obscure the broader point: Our due process precedents, even our "substantive due process" precedents, do not support *any* right to informational privacy.

[R]espondents challenge the Government's *collection* of their private information. But the Government's collection of private information is regulated by the Fourth Amendment, and "[w]here a particular Amendment provides an explicit textual source of constitutional protection against a particular sort of government behavior, that Amendment, not the more generalized notion of substantive due process, must be the guide for analyzing these claims."

The Court's sole justification for its decision to "assume, without deciding" is that the Court made the same mistake before—in two 33–year–old cases, *Whalen v. Roe* (1977) and *Nixon v. Administrator of General Services* (1977). But *stare decisis* is simply irrelevant when the pertinent precedent assumed, without deciding, the existence of a constitutional right. Here, however, the Court actually *applies* a constitutional informational privacy standard without giving a clue as to the rule of law it is applying.

It provides no guidance whatsoever for lower courts. Consider the sheer multiplicity of unweighted, relevant factors alluded to in today's opinion:

- It is relevant that the Government is acting "in its capacity 'as proprietor' and manager of its 'internal operation.'" Of course, given that we are told neither what the appropriate standard should be when the Government is acting as regulator nor what the appropriate standard should be when it is acting as proprietor, it is not clear *what* effect this fact has on the analysis; but at least we know that it is *something*.
- History and tradition have some role to play, but how much is uncertain. The Court points out that the Federal Government has been conducting investigations of candidates for employment since the earliest days; but on the other hand it acknowledges that extension of those investigations to employees of contractors is of very recent vintage.
- The contract employees are doing important work. They are not mere janitors and maintenance men; they are working on a $568 million observatory. Can it possibly be that the outcome of today's case would be different for background checks of lower-level employees? In the spirit of minimalism we are never told.
- Questions about drug treatment are (hypothetically) constitutional because they are "reasonable," "useful," and "humane." And questions to third parties are constitutional because they are "appropriate" and "pervasiv[e]." Any or all of these adjectives may be the hypothetical standard by which violation of the hypothetical constitutional right to "informational privacy" is evaluated.
- The Court notes that a "'statutory or regulatory duty to avoid unwarranted disclosures' *generally* allays these privacy concerns," but it gives no indication of what the exceptions to this general rule might be. It then discusses the provisions of the Privacy Act in detail, placing considerable emphasis on the limitations imposed by NASA's routine-use regulations. From the length of the discussion, I would bet that the Privacy Act is necessary to today's holding, but how much of it is necessary is a mystery.

In future cases filed under 42 U.S.C. § 1983 in those circuits that recognize (rather than merely hypothesize) a constitutional right to "informational privacy," lawyers will always (and I mean *always*) find some way around today's opinion: perhaps the plaintiff will be a receptionist or a janitor, or the protections against disclosure will be less robust. And oh yes, the fact that a losing defendant will be liable not only for damages but also for attorney's fees under § 1988 will greatly encourage lawyers to sue, and defendants—for whom no safe harbor can be found in the many words of today's opinion—to settle. These plaintiffs' claims have failed today, but the Court makes a generous gift to the plaintiffs' bar.

Justice THOMAS, concurring in the judgment.

I agree with Justice SCALIA that the Constitution does not protect a right to informational privacy. No provision in the Constitution mentions such a right.

Notes

1. Four years after *Nelson*, what the majority dismissed as "a possibility" came to pass in the form of one of the largest data breaches of government data in U.S. history. In June 2015, the Office of Personnel Management disclosed that a cyberattack compromised the records of 21.5 million individuals.[134] About 1.8 million of these victims were not background investigation applicants but individuals living with an applicant, such as a spouse.[135] A 2016 congressional committee report later revealed that the compromised data included forms which asked intimate questions concerning an employee's mental health treatment history, illegal consumption of drugs or controlled substance, and whether an employee "experienced financial problems due to gambling."[136] The committee found that the stolen background investigation data presented a "counterintelligence value" that "cannot be overstated, nor will it ever be fully known."
2. Our days of being uncertain about the status of the constitutional right to information privacy are, in the words of the poet, "coming to a middle." Whatever one might think of Justice Scalia's general jurisprudence, he does a good job here skewering the Court's lack of clarity. Is there such a right? How should we assess it?
3. Lower courts are split on the right to information privacy. The Third Circuit developed a seven-part test to determine whether the government could acquire records like those at issue in *Whalen*.[137] This test, broadly speaking, balances the magnitude of the privacy invasion (including the harm likely to be inflicted if the data is subsequently released and the extent of the data-security measures) against the extent of the state's interest.[138] The Second, Fifth, Seventh, and Ninth Circuits have also recognized the right to information

---

[134] Lee Tien, *We Told You So: OPM Data Breach Reveals Not Only Lame Security But Weak Legal Protections–And It's Time to Revisit Both*, Electronic Frontier Foundation (July 16, 2015), https://www.eff.org/deeplinks/2015/07/we-told-you-so-opm-data-breach-reveals-not-only-lame-data-security-weak-legal.

[135] Lisa Rein & Andrea Peterson, *A breakdown of what is known about the compromise so far*, The Washington Post (July 10, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/what-you-need-to-know-about-the-hack-of-government-background-investigations/

[136] Committee on Oversight and Government Reform, *The OPM Data Breach: How Government Jeopardized Our National Security for More Than a Generation* v, vi, https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

[137] *U.S. v. Westinghouse Elec. Corp.*, 638 F.2d 570, 578 (3d Cir. 1980).

[138] *See id.* (providing the following factors to be considered when deciding if an intrusion is justified: (1) the "type of record requested," (2) "the information it does or might contain," (3) "the potential for harm in any subsequent nonconsensual disclosure," (4) the injury a disclosure would cause to the relationship that generated the record, (5) the "adequacy of safeguards to prevent unauthorized disclosure," (6) "the degree of need for access," and (7) whether there is a public policy reason or statutory mandate militating toward access.); *Doe v. Se. Pa. Transp. Auth.*, 72 F.3d 1133, 1135–38 (3d Cir. 1995) (applying this test to the disclosure of an employee's HIV status).

privacy in some form,[139] but the Sixth Circuit has been more cautious and the D.C. Circuit has questioned whether there is a constitutional right to information privacy at all.[140]

2) Circuit level reactions to uncertainty

The status of the right to information privacy is uncertain after *Nelson* (and potentially even more so after *Dobbs*). The below Eighth Circuit opinion highlights the difficulties raised by the Supreme Court's unclear guidance. It also introduces two key concepts: Section 1983 and the doctrine of qualified immunity.

42 U.S.C. § 1983 provides a civil cause of action against individuals who violate the constitutional rights of others while acting "under color of" state law. So, a state police officer, county building inspector, or town garbage collector could all potentially violate Section 1983 if, in the course of their duties, they deprive an individual of "any rights, privileges, or immunities secured by the Constitution and laws."[141] Notably Section 1983 does not apply to federal officials; their liability is governed by the ever-shrinking *Bivens* doctrine.[142]

Holding either state or federal agents civilly liable is notoriously difficult. A federal courts or federal jurisdiction class would review the host of ways such actors might have immunity from damages. The only important one for this case is the doctrine of qualified immunity, which protects state and local officials, including law enforcement officers, from individual liability unless the official violated a "clearly established" constitutional right. "Clearly established" means that, at the time of the official's conduct, the law was sufficiently clear that every reasonable official would understand that what he or she is doing is unconstitutional. According to the Supreme Court, qualified immunity protects all except the plainly incompetent or those who knowingly violate the law.

Dillard v. O'Kelley, 961 F.3d 1048 (8th Cir. 2020)

LOKEN, Circuit Judge

Jill Dillard, Jessa Seewald, Jinger Vuolo, and Joy Duggar ("Plaintiffs") rose to prominence as members of the cast of "19 Kids and Counting," a television show about Jim Bob Duggar, his wife Michelle, and their nineteen children in Washington County, Arkansas. In 2015, the City of Springdale Police Department ("SPD") and the Washington County Sheriff's Office ("WCSO"), responding to a tabloid's request under the Arkansas Freedom of Information Act ("FOIA"), released redacted copies of reports of a 2006 investigation into sexual misconduct by the Duggars' oldest child, Josh Duggar, which included interviews of Plaintiffs, who were minors at the time. Despite redactions, social media users identified Plaintiffs as the victims of Josh's reported sexual abuse. The resulting negative publicity brought about the show's demise, and then, this lawsuit.

---

[139] *See, e.g.*, *Barry v. City of N.Y.*, 712 F.2d 1554, 1559 (2d Cir. 1983); *Fadjo v. Coon*, 633 F.2d 1172, 1176 (5th Cir. 1981); *Coffman v. Indianapolis Fire Dep't*, 578 F.3d 559, 566 (7th Cir. 2009); *In re Crawford*, 194 F.3d 954, 959 (9th Cir. 1999).

[140] *See J.P. v. DeSanti*, 653 F.2d 1080, 1089–90 (6th Cir. 1981) ("We do not view the discussion of confidentiality in *Whalen v. Roe* as . . . creating a constitutional right to have all government action weighed against the resulting breach of confidentiality."); *Am. Fed'n of Gov't Emps., AFL–CIO v. Dep't of Hous. & Urban Dev.*, 118 F.3d 786, 791 (D.C. Cir. 1997).

[141] In practice, any damages assessed against a government actor are almost always paid by the government rather than by the individual themselves.

[142] *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*, 403 U.S. 388 (1971). *Bivens* allows for a federal cause of action for money damages against federal officials for violating constitutional rights under color of law. In general, the Supreme Court has been reluctant to expand *Bivens* actions. See, e.g., *Egbert v. Boule*, 596 U.S. 482 (2022)

Plaintiffs sued the City, the County, and several of their employees, asserting claims under 42 U.S.C. § 1983 and the Arkansas Civil Rights Act, along with state law tort claims for the tort of outrage and invasion of privacy. As relevant here, Plaintiffs alleged that Springdale Police Chief Kathy O'Kelley, Springdale City Attorney Ernest Cate, and WCSO Enforcement Major Rick Hoyt ("individual defendants" or "Defendants") violated Plaintiffs' Fourteenth Amendment rights to informational privacy by disclosing the redacted reports to the media.

Plaintiffs' Complaint alleges that on December 7, 2006, the Arkansas State Police ("ASP") Child Abuse Hotline received an anonymous tip that Josh Duggar had molested his younger sisters Jill, Jessa, Jinger, and Joy, along with another unnamed individual, at various times in 2002 and 2003. SPD opened an investigation and requested an "agency assist" from WCSO. An ASP investigator questioned Plaintiffs about the assaults; they were promised their answers would remain confidential. A WCSO detective interviewed Jim Bob and Michelle Duggar, who acknowledged the allegations and identified the victims, location, and frequency of Josh's sexual misconduct. WCSO documented the Duggar interview in an Incident Report; SPD summarized both the Duggar and sibling interviews in an Offense Report. Based on the interviews, SPD submitted an affidavit to the Washington County Family in Need of Services Division and the Washington County Prosecutor's Office. No criminal charges were filed, nor were the allegations made public.

The Complaint further alleges that on May 15, 2015, a tabloid called *In Touch Weekly* submitted FOIA requests to the SPD and the WCSO, seeking files related to Jim Bob Duggar, Michelle Duggar, Josh Duggar, and multiple addresses. The request stated that *In Touch* had reason to believe the agencies had filed reports regarding the sexual assaults. The Arkansas FOIA required a response by May 20. On May 19, before SPD or WCSO responded, *In Touch Weekly* published an online article titled, "'19 Kids and Counting' Son Named in Underage Sex Probe." The article stated that "multiple sources who have seen the police report and are familiar with the case" told the tabloid that police had investigated an alleged sexual assault. "Josh was brought into the Arkansas State Police by his father," after Jim Bob "caught [Josh] leaving a young girl's bedroom and 'learned something inappropriate happened.'" "Rumors about Josh have swirled for years," the article continued; "*In Touch's* investigation has uncovered the secret he has been hiding."

According to the Complaint, appellants O'Kelley and Cate "directed, oversaw, and approved" SPD's FOIA response. Officials suspected that employees were leaking details of the investigation to the media; O'Kelley worried that her department would "soon end up in the tabloids" and become the target of "worldwide media attention." Without seeking guidance from the Arkansas Municipal League or the City's child services department, O'Kelley and Cate decided to release a redacted Offense Report in response to the FOIA request and "rushed to prepare" the report. Appellant Hoyt "organized, oversaw, and approved" WSCO's redactions, while County Attorney Steve Zega "oversaw, counseled, and approved" the release of the report. On the evening of the May 20 deadline, O'Kelley received the redacted SPD Offense Report and sent it to *In Touch Weekly* and a local news organization. The next day, Hoyt and Zega directed WCSO employees to mail the redacted Incident Report to *In Touch Weekly*.

The redactions did not prevent identification of Plaintiffs as four of Josh's victims. Both reports included Jim Bob and Michelle Duggar's names, their current and former addresses, and "other personal details" about each individual victim. The Offense Report contained "full descriptions" of the victim interviews, and the Complaint alleges that Plaintiffs were "obviously identifiable." The Incident Report "expressly identified one of Josh's victims as his then 5-year-old sister." In response to a request from Cate, the Arkansas Municipal League advised that Arkansas law prohibited disclosing the identity of sex crime victims. O'Kelley then asked *In Touch Weekly* to refrain from using Jim Bob and Michelle Duggar's names and accept a different version of the SPD report. Instead, the tabloid published the original Offense Report with an article titled, "Bombshell Duggar Police Report: Jim Bob Duggar Didn't Report Son Josh's

Alleged Sex Offenses For More Than A Year," and reporting that "explosive new information is contained in a Springdale, Ark. police report obtained by *In Touch* magazine." The article revealed details of the sexual assaults, including that some occurred while the victims were sleeping, one victim was fourteen at the time, and the victims forgave Josh after he apologized.

The Complaint alleges a "public backlash" against the disclosures. Based on interview details, social media users identified Plaintiffs as the victims. Some commentators expressed sympathy, others "chastised [Plaintiffs'] personal decision to forgive their brother," while others "reveled in the *ad hoc* disclosure of the lurid details" and subjected Plaintiffs to "spiteful and harsh comments and harassment." In response to Joy Duggar's motion, a state court judge ordered the Offense Report expunged from the public record, ordered all copies destroyed, and ruled that interviews and information about the sexual assaults were not subject to FOIA disclosure. Undeterred, *In Touch Weekly* continued to post copies of the Offense Report and expanded its coverage of the scandal. A June 3 article highlighted a "new report . . . from the Washington County Sheriff's Office," which had "fewer redactions" and "show[ed] the extent of Josh's abuse." A June 15 article quoted an "insider" as saying, "The four Duggar girls 'forgave' Josh for his sins, but that's not how you get over sexual abuse." The Complaint alleges that publicizing their trauma subjected Plaintiffs and their families "to extreme mental anguish and emotional distress."

The issue presented by this interlocutory appeal is whether individual Defendants O'Kelley, Cate, and Hoyt are entitled to qualified immunity from Plaintiffs' § 1983 damage claims. Qualified immunity shields public officials from liability for civil damages if their conduct did not "violate clearly established statutory or constitutional rights of which a reasonable person would have known." *Harlow v. Fitzgerald* (1982). The Supreme Court has repeatedly "stressed the importance of resolving immunity questions at the earliest possible stage in litigation." *Pearson v. Callahan* (2009). To defeat a motion to dismiss based on qualified immunity, Plaintiffs must "plead[ ] facts showing (1) that the official violated a statutory or constitutional right, and (2) that the right was 'clearly established' at the time of the challenged conduct." *Ashcroft v. al-Kidd* (2011).

Qualified immunity "protects all but the plainly incompetent or those who knowingly violate the law." *Mullenix v. Luna* (2015). Thus, "[a] clearly established right is one that is sufficiently clear that every reasonable official would have understood that what he is doing violates that right." The Supreme Court "has repeatedly told courts . . . not to define clearly established law at a high level of generality." *Kisela v. Hughes* (2018). Rather, we look for a controlling case or "a robust consensus of cases of persuasive authority." *Al-Kidd*. There need not be a prior case directly on point, but "existing precedent must have placed the statutory or constitutional question beyond debate."

Despite the Court's inconclusive acknowledgment of a constitutional right it held not violated, a majority of the courts of appeals interpreted *Whalen* and *Nixon* as recognizing a constitutional right to the privacy of medical, sexual, financial, and other categories of highly personal information, grounded in the Fourteenth Amendment right to substantive due process. Panels of this court followed suit.

Although *Nelson* left the issue unresolved, it confirmed that our court and other circuits erred in reading inconclusive statements in *Whalen* and *Nixon* as Supreme Court recognition of a substantive due process right to informational privacy.

Although *Whalen* and *Nixon* did not involve alleged wrongful disclosures of private information, a number of our pre-*Nelson* decisions extended their interpretation of those decisions to disclosures of "inherently private" information that is "either a shocking degradation or an egregious humiliation . . . or a flagrant breach of a pledge of confidentiality which was instrumental in obtaining the personal information." *Eagle v. Morgan* (8th Cir. 1996). However, although we considered a wide variety of disclosures, in each case we concluded

that the alleged right had not been violated. *See Cooksey v. Boyer* (8th Cir. 2002) (disclosure of police chief's treatment for stress); *Riley v. St. Louis Cty. of Mo.* (8th Cir. 1998) (release of photo of son's body following suicide); *Wade v. Goodwin* (8th Cir. 1988) (disclosure of list of "survivalists" denoting membership in organizations like the Ku Klux Klan). Indeed, in *Eagle*, we reversed the denial of qualified immunity, noting "that the exact boundaries of this right are, to say the least, unclear." To the extent these cases read *Whalen* and *Nixon* as recognizing the right to informational privacy, *Nelson* makes clear they were wrong to do so. The disclosures in this case occurred years after the decision in *Nelson*, and we have not revisited the issue. The resulting legal uncertainty surely means the alleged constitutional right to informational privacy is not "beyond debate" in the Eighth Circuit.

[T]he uncertain status of the right to informational privacy means that Defendants are entitled to qualified immunity. If a right does not clearly exist, it cannot be clearly established.

GRASZ, Circuit Judge, with whom SMITH, Chief Judge, joins, concurring in part and concurring in the result.

The constitutional right to informational privacy in the Eighth Circuit is dead.[3] Some believe it never lived. In any event, in this age of digital information, where the government may possess massive amounts of personal data, the protection of twenty-two million people from wrongful disclosure of intimately private information by government officials now lies squarely in the hands of the state legislatures in Arkansas, Iowa, Minnesota, Missouri, Nebraska, North Dakota, and South Dakota. Perhaps that is where it belonged from the start, given that the federal constitution is silent on the matter and the United States Supreme Court has yet to conclude that a constitutional right to informational privacy exits.

While the demise of informational privacy as a constitutional right in this circuit may be appropriate, we should at least recognize this was not an academic exercise to the plaintiffs. The court has concluded that the Arkansas public officials here, who are alleged to have callously revealed intimate and humiliating personal information of young sexual assault victims to a tabloid under highly suspicious circumstances, are exempt from liability because of qualified immunity.[5] The court does so, in part, based on the proposition that a constitutional right not definitively recognized by the Supreme Court cannot be "clearly established" for purposes of qualified immunity analysis. While this reasoning may have facial appeal, it is simply not true that a right established in circuit precedent cannot be "clearly established" for purposes of qualified immunity even in the absence of definitive Supreme Court precedent. Indeed, many other circuit courts would likely be quite surprised by this holding.[6] Regardless, today's decision means future litigants have no recourse in this circuit under 42 U.S.C. § 1983 for informational privacy violations.

I remain of the view that the panel below was bound to follow this court's opinions in *Cooksey v. Boyer* (8th Cir. 2002), *Eagle v. Morgan* (8th Cir. 1996), and *Alexander v. Peffer* (8th

---

[3] Although a litigant might, in theory, still attempt a facial challenge to a statute or regulation, or seek to enjoin the prospective release of information, the retroactive enforcement of any right to informational privacy under 42 U.S.C. § 1983 is now effectively precluded.

[5] Like informational privacy, qualified immunity is a textually invisible right.

[6] Several of our sister circuits have denied qualified immunity while finding the right to informational privacy was clearly established. *See Anderson v. Blake*, 469 F.3d 910, 912, 917 (10th Cir. 2006) (video of rape victim's assault disclosed by police officer); *Sterling v. Borough of Minersville*, 232 F.3d 190, 192 (3d Cir. 2000) (threat to disclose arrestee's sexual orientation); *Denius v. Dunlap*, 209 F.3d 944, 956–57 (7th Cir. 2000) (medical information of a teacher); *James v. City of Douglas, Georgia*, 941 F.2d 1539, 1540–41 (11th Cir. 1991) (police officer viewed and allowed other people to view video of informant and suspect engaging in sexual activity). Other circuits have recognized the right and found violations. *See Tucson Woman's Clinic v. Eden*, 379 F.3d 531, 551 (9th Cir. 2004) (medical records); *Doe v. City of New York*, 15 F.3d 264, 267 (2d Cir. 1994) (recognizing the constitutional right to confidentiality of a HIV diagnosis).

Cir. 1993), in which we recognized and narrowly defined the right to informational privacy. However, I agree with the en banc court that the foundation of those cases is gone. And today's decision has effectively negated them. ("To the extent these cases read *Whalen* and *Nixon* as recognizing the right to informational privacy . . . they were wrong to do so."). With no right to informational privacy recognized in this circuit, the appellants cannot, as a matter of law, prevail against the assertion of qualified immunity. They must instead look to state law for relief.

KELLY, Circuit Judge, concurring in part and dissenting in part.

In 2006, Plaintiffs provided private and intimate details regarding their childhood sexual abuse to government officials under a promise of confidentiality. More than eight years later, government officials broke that promise and disclosed this sensitive information to a tabloid without Plaintiffs' consent. Because I believe this violated Plaintiffs' clearly established right to privacy, I respectfully dissent.

The issue in this appeal is whether a reasonable government official in the Eighth Circuit would have understood that disclosing to a tabloid private information regarding childhood sexual abuse would violate the constitutional right to privacy. This raises two basic questions: (1) whether this court's caselaw, prior to *NASA v. Nelson* (2011), provided fair notice that publicly disclosing this information would violate the constitutional right to privacy; and (2) if so, whether a government official could have reasonably believed that Nelson had undermined that caselaw.

I agree with the district court and the panel that our pre-*Nelson* caselaw clearly established that the government's disclosure of this sensitive information would violate the constitutional right to privacy. This court has repeatedly stated, in no uncertain terms, that "the right to privacy embodied in the fourteenth amendment" protects "an individual's interest in avoiding disclosures of personal matters." *Alexander v. Peffer* (8th Cir. 1993). Following other circuits, we have held that to violate an individual's constitutional right of privacy "the information disclosed must be either a shocking degradation or an egregious humiliation of her to further some specific state interest, or a flagrant bre[a]ch of a pledge of confidentiality which was instrumental in obtaining the personal information."

Until this case, we had not been presented with a factual scenario that satisfied this exacting standard. But in my view, we had provided fair notice to government officials in the Eighth Circuit that the public disclosure of "highly personal matters representing the most intimate aspects of human affairs," that is "either a shocking degradation or an egregious humiliation . . . , or a flagrant breach of a pledge of confidentiality," violates the constitutional right to privacy. As a result, government officials in the Eighth Circuit are not entitled to qualified immunity for such disclosures.

Four judges have decided that Plaintiffs' constitutional right against the disclosure of this information was clearly established. The district court reasoned that

> taking the facts alleged in the Complaint as true, any reasonable person in the position to make these disclosures would have understood that these disclosures would be published, would cause a national scandal, would be a "shocking degradation" or "egregious humiliation" for the Plaintiffs, that the Plaintiffs had a "legitimate expectation" of confidentiality in these materials, and that disclosing these materials would therefore violate the Plaintiffs' constitutional right to privacy.

Dillard v. City of Springdale (W.D. Ark. Sept. 29, 2017). A unanimous panel of this court agreed, concluding that:

> The particular facts alleged here are not near the periphery of the right to privacy but at its center. Certainly, allegations of incestuous sexual abuse implicate "the

> most intimate aspects of human affairs" and are "inherently private." The content and circumstances of these disclosures do not just meet the standard of "shockingly degrading or egregiously humiliating," they illustrate them. And releasing insufficiently redacted reports detailing minors' sexual abuse to a tabloid, notwithstanding promises that these reports would remain private, is "a flagrant breach of a pledge of confidentiality."
>
> *Dillard v. City of Springdale* (8th Cir. 2019) (cleaned up).

These decisions are well-supported. Other courts have similarly concluded that a reasonable government official would have notice that the constitutional right to privacy protects against the government's disclosure of the details of sexual abuse. *See Sealed Plaintiff No. 1 v. Farber* (2d Cir. 2007) (affirming the denial of qualified immunity and noting that "a person's status as a juvenile sex abuse victim is clearly the type of 'highly personal' information that we have long recognized as protected by the Constitution from governmental dissemination"); *Anderson v. Blake* (10th Cir. 2006) (affirming the denial of qualified immunity because plaintiff had a constitutionally protected privacy interest in a rape video and was not required, at the motion-to-dismiss stage, to disprove every possible compelling interest the government might assert); *Bloch v. Ribar* (6th Cir. 1998) (concluding that "a rape victim has a fundamental right of privacy in preventing government officials from gratuitously and unnecessarily releasing the intimate details of the rape where no pen[o]logical purpose is being served" and stating that, as of September 1998, public officials in the Sixth Circuit were "on notice that such a privacy right exists"); *Stafford-Pelt v. California* (N.D. Cal. June 20, 2005) (denying qualified immunity because plaintiff had plausibly alleged that disclosing partially redacted reports detailing her allegations of sexual abuse against her half-brother violated her clearly established right to privacy). I believe our pre-*Nelson* precedent dictates this same result.

The question then becomes whether our precedent was undermined, such that the rule in this circuit would not have been clear to a reasonable official, by the Supreme Court's decision in *Nelson*. In that case, the Court "assume[d], without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*." And it explained that, contrary to the interpretation adopted by most circuits, this was "the same approach . . . the Court took more than three decades ago in *Whalen* and *Nixon*."

In the court's view, "Nelson raises an essential question: whether a right the Supreme Court has only assumed may exist, and this court has never held to be violated, can be a clearly established constitutional right." Relying on *Reichle v. Howards* (2012), the court answers this question in the negative, reasoning that "the uncertain status of the right to informational privacy means that Defendants are entitled to qualified immunity." I disagree.

I do not agree that *Nelson's* effect on our right-to-privacy caselaw is similar to *Hartman's* effect on the Tenth Circuit's retaliatory-arrest caselaw. Unlike *Hartman v. Moore* (2006), which was intended to resolve a circuit split and abrogate contrary circuit authority, *Nelson* purported to leave the state of the law intact. The Court expressly acknowledged that, after *Whalen* and *Nixon*, different circuits had adopted different interpretations of when the disclosure of private information by government officials would violate the right to privacy, and the Court declined to decide which circuit's caselaw was correct.

Notes

1. The challenge in qualified immunity cases is not just showing that the plaintiff should win now, but that it was clear the plaintiff should win prior to this case. This makes it very difficult to have the law progress as no plaintiff should ever benefit from a novel finding of liability. This makes some amount of sense if one thinks about the perspective of the

government agent—if they reasonably thought that something was legal, they should not be made to pay. But it is little comfort to the plaintiff/victim.

Not every circuit is as strict in its understanding of qualified immunity as was the Eighth Circuit here. Consider the below earlier case from the Third Circuit.

Sterling v. Borough of Minersville, 232 F.3d 190 (3rd Cir. 2000)

MANSMANN, Circuit Judge.

This interlocutory appeal arises from a denial of the defendants' motion for summary judgment on qualified immunity grounds. At issue is whether police officers' threat to disclose the suspected sexual orientation of an arrestee to his family member violated the young man's constitutional right to privacy. We will affirm the order of the District Court because the law is clearly established that matters of personal intimacy are protected from threats of disclosure by the right to privacy and at least one of the officers involved was aware that his conduct was knowingly violative of that right.

On April 17, 1997, 18–year old Marcus Wayman and a 17–year old male friend were parked in a lot adjacent to a beer distributor. The car and its occupants were observed by the defendant police officer, F. Scott Wilinsky. Wilinsky was concerned about previous burglaries of the beer distributor and was suspicious of the fact that the headlights on the car were out. Wilinsky called for back-up and, shortly thereafter, Officer Thomas Hoban, the second defendant, arrived at the scene.

The officers' investigation did not show any sign of a break-in at the business, but it was apparent to the officers that the young men had been drinking alcohol. The boys were also evasive when asked what they were doing in the parking lot. When an eventual search uncovered two condoms, Wilinsky questioned whether the boys were in the parking lot for a sexual assignation. Wilinsky testified that both Wayman and his companion eventually acknowledged that they were homosexuals and were in the parking lot to engage in consensual sex, but we note that the 17–year old denied making such admissions.

The two boys were arrested for underage drinking and were taken to the Minersville police station. At the station, Wilinsky lectured them that the Bible counseled against homosexual activity. Wilinsky then warned Wayman that if Wayman did not inform his grandfather about his homosexuality that Wilinsky would take it upon himself to disclose this information. After hearing this statement, Wayman confided to his friend that he was going to kill himself. Upon his release from custody, Wayman committed suicide in his home.

Wayman's mother, Madonna Sterling, as executrix of her son's estate, filed suit under 42 U.S.C. § 1983 against the Borough of Minersville, Wilinsky and Hoban, as individuals and in their capacity as police officers, and the Chief of Police of Minersville. The complaint alleged that the officers and the borough violated Wayman's Fourth Amendment right against illegal arrest, his Fourteenth Amendment rights to privacy and equal protection and the laws and the Constitution of the Commonwealth of Pennsylvania.

We have previously set forth the analytical framework for deciding qualified immunity claims. First, we must determine if the plaintiff has alleged a deprivation of a clearly established constitutional right. A right is clearly established if its outlines are sufficiently clear that a reasonable officer would understand that his actions violate the right. If a violation exists, the immunity question focuses on whether the law is established to the extent that "the unlawfulness of the action would have been apparent to a reasonable official."

We first ask whether Wayman had a protected privacy right concerning Wilinsky's threat to disclose his suspected sexual orientation. If the right exists, we then query whether it was clearly established at the time of its alleged violation.

In *Griswold v. Connecticut* (1965), the Supreme Court first acknowledged the individual's constitutional right to privacy. In *Griswold*, the Court declared that a state law prohibiting use of contraceptives by married couples was unconstitutional because it violated the right to privacy as gleaned from the penumbra of rights established by the Bill of Rights.

The boundaries of the right to privacy, however, have not been clearly delineated.[2] [Review of *Griswold*, *Eisenstadt*, and *Roe* omitted].

The constitutional right to privacy was further refined in *Whalen v. Roe* (1977). In *Whalen*, the constitutionality of a New York statute which required that the state be provided with a copy of prescriptions for certain drugs was challenged by physicians and patients. While the statute's validity was ultimately upheld, the Court held that the constitutional right to privacy respects not only an individual's autonomy in intimate matters, but also an individual's interest in avoiding divulgence of highly personal information.

We recognize that the Supreme Court has not definitively extended the right to privacy to the confidentiality of one's sexual orientation. Indeed, a later case gives us pause. In *Bowers v. Hardwick* (1986), the Supreme Court overturned a decision of the Court of Appeals of the Eleventh Circuit that had invalidated a Georgia statute that made consensual homosexual sodomy a criminal offense. The majority rejected the claim that the Constitution confers a "fundamental right to homosexuals to engage in consensual sodomy."

While *Bowers* indicates that the Court is resistant to bestowing the protection of the Constitution on some sexual behavior, its ruling focused on the practice of homosexual sodomy and is not determinative of whether the right to privacy protects an individual from being forced to disclose his sexual orientation. In other words, the decision did not purport to punish homosexual status. Such a determination would in fact be contrary to the Court's holding in *Robinson v. California* (1962), that the Eighth and Fourteenth Amendments forbid punishment of status as opposed to conduct. We do not read *Bowers* as placing a limit on privacy protection for the intensely personal decision of sexual preference.

Our jurisprudence takes an encompassing view of information entitled to a protected right to privacy. "[T]he right not to have intimate facts concerning one's life disclosed without one's consent . . . is a venerable one whose constitutional significance we have recognized. . . . " *Bartnicki v. Vopper* (3d Cir. 1999).

First, in *United States v. Westinghouse Electric Corp.* (3d Cir. 1980), we held that private medical information is "well within the ambit of materials entitled to privacy protection," in part because it concerns intimate facts of a personal nature. We cautioned, however, that the right is not absolute. Public health or like public concerns may justify access to information an individual may desire to remain confidential. In examining right to privacy claims, we, therefore, balance a possible and responsible government interest in disclosure against the individual's privacy interests..

In *Fraternal Order of Police v. City of Philadelphia* (3d Cir. 1987), we held that questions posed concerning medical, financial and behavioral information relating to whether police officer applicants were capable of working in stressful and dangerous positions did not unconstitutionally infringe on the applicant's privacy rights, but determined that there were inadequate safeguards on unnecessary disclosure of the information obtained. We observed that "[i]t would be incompatible with the concept of privacy to permit protected information . . . to be publicly disclosed." In performing the necessary balancing inquiry, we looked to the

---

[2] The privacy right has been extended to activities relating to marriage, *Loving v. Virginia* (1967); procreation, *Skinner v. Oklahoma* (1942); contraception, *Eisenstadt v. Baird* (1972); family relationships, *Prince v. Massachusetts* (1944); child rearing and education, *Pierce v. Society of Sisters* (1925).

individual's privacy expectation and concluded that "[t]he more intimate or personal the information, the more justified is the expectation that it will not be subject to public scrutiny."

Next, in *Doe v. Southeastern Pennsylvania Transportation Authority* (3d Cir. 1995), a public employee brought a section 1983 action for violations of his right to privacy when the employer discovered, through records of drug purchases made through the employee health program, that the employee had AIDS. After weighing certain factors to determine whether the disclosure constituted an actionable invasion of privacy, we determined that the public employer's need to access the prescription records for purposes of monitoring the health plan outweighed the employee's interest in keeping his drug purchases confidential. We arrived at this conclusion, however, only after identifying the government's interest in the information as "genuine, legitimate and compelling."

Most recently, in *Gruenke v. Seip* (3d Cir. 2000), a high school swim team coach, suspecting that a teenage team member was pregnant, required the young woman to take a pregnancy test. The young woman and her mother filed a section 1983 action claiming *inter alia* that the pregnancy test unconstitutionally interfered with the daughter's right to privacy regarding personal matters. We decided that the daughter's claim "falls squarely within the contours of the recognized right of one to be free from disclosure of personal matters as outlined in *Whalen v. Roe*" and held that the fact that the coach compelled the student to take the test, coupled with an alleged failure to take appropriate steps to keep the information confidential infringed the girl's right to privacy. Significant to today's matter, we determined that this type of conduct was not objectively reasonable under the law and could not entitle the coach to immunity from suit.

We thus carefully guard one's right to privacy against unwarranted government intrusion. It is difficult to imagine a more private matter than one's sexuality and a less likely probability that the government would have a legitimate interest in disclosure of sexual identity.

The zone of privacy, while clearly established in matters of personal intimacy, is not absolute. If there is a government interest in disclosing or uncovering one's sexuality that is "genuine, legitimate and compelling," *Doe v. SEPTA*, then this legitimate interest can override the protections of the right to privacy. In this instance, however, no such government interest has been identified. Indeed, Wilinsky conceded he would have no reason to disclose this type of sensitive information.

We turn then to whether Wilinsky should have known that his conduct, as described by the plaintiff, violated clearly established law. As previously discussed, by Wilinsky's own acknowledgment, disclosure of Wayman's suspected homosexuality would be a matter of private concern. Wilinsky stated that because Wayman was 18, there was no reason for him to interfere with Wayman's family's awareness of his sexual orientation. In addition, Wilinsky testified that he did not include suspicion of homosexual activity in his police report because of the confidential nature of the information. Obviously, then, Wilinsky was aware that one's sexual orientation is intrinsically personal and no compelling reason to disclose such information was warranted. Because the confidential and private nature of the information was obvious, and because the right to privacy is well-settled, the concomitant constitutional violation was apparent notwithstanding the fact that the very action in question had not previously been held to be unlawful. Accordingly, Wilinsky could not reasonably have believed that his questioned conduct was lawful in light of the established law protecting privacy rights.

STAPLETON, Circuit Judge, dissenting:

I respectfully dissent.

In order for law to be "clearly established" for purposes of qualified immunity, there must be pre-existing authority which rules out the possibility that a reasonable official in the

defendant's position could have believed his conduct to be lawful. Here, prior to the events giving rise to this case, there was no Supreme Court case law addressing either the issue of whether there is a constitutionally protected right of privacy in one's sexual orientation, or the issue of whether a mere threat to disclose constitutionally protected private information can constitute a constitutional tort.

Before elaborating on our differences, I note my agreement with much that the Court has today said. Though we have not addressed the issue before, I agree that, based on the precedents of this Court, Wayman did possess a privacy interest in his sexual orientation. Our previous decisions in *Westinghouse* and *Fraternal Order of Police* have understood the right to privacy to encompass all "intimate facts of a personal nature." I think it fair to say that our society regards a person's sexual orientation as intimate information of a personal nature and, accordingly, recognizes a reasonable and legitimate expectation of privacy in that information.

The alleged action of Wilinsky primarily at issue here is his threat to disclose private information. It is clear that while Officer Wilinsky threatened to disclose Wayman's suspected sexual orientation, he did not in fact do so. Even so, I am in agreement with the Court that Wilinsky's threat to disclose Wayman's suspected sexual orientation violated the Constitution. I reach this conclusion, however, by a different route than the Court. I believe that a threat to disclose private information violates the constitutional right to privacy only where, as here, an officer with no legitimate interest in effecting disclosure makes a threat, the intended and foreseeable effect of which is involuntary self-disclosure.

Essentially a blackmail mechanism, Wilinsky's "tell now or I'll tell later" threat had the foreseeable effect of forcing disclosure by Wayman without any further action on the part of Wilinsky. It would make little sense to condone an officer's acts effecting disclosure simply because the victim is made the instrument of the disclosure. It makes more sense to examine the culpability of the conduct and ask whether an officer completed steps reasonably designed to effect disclosure with the intent that disclosure would result. In short, I believe Wilinsky's threat itself was a violation of Wayman's right to privacy because Wilinsky, acting as a state officer, knowingly engaged in conduct reasonably calculated to effect the involuntary disclosure of Wayman's sexual orientation.

Thus, I agree with the Court's decision that a constitutional violation occurred. I part ways with my colleagues, however, on whether the unconstitutionality of Wilinsky's conduct was clearly established by the pre-existing case law.

First, a person's right to privacy in his or her sexual orientation simply was not clearly established in April of 1997. Only one opinion directly addressing the issue existed at the time of Wilinsky's conduct, and that opinion held that no right to privacy exists in a person's sexual orientation. *See Walls v. City of Petersburg* (4th Cir. 1990) (rejecting, on the authority of *Bowers v. Hardwick* (1986), the proposition that a city employee's right to privacy was violated by her being requiring to state whether she had "ever had sexual relations with a person of the same sex"). With the relevant case law in this state, I am unable to conclude that no reasonable officer in Wilinsky's position could have believed his conduct to be consistent with the Constitution.

Notes

1. Notice that this case came between *Bowers* and *Lawrence*, and that the majority needed to do some very careful writing to get around what it plainly believed was the mistaken holding of *Bowers*.
2. How consistent is this case's approach to qualified immunity compared to that of *Dillard*? When should we expect a plaintiff to win an information privacy challenge, and how much does it depend on circuit?

VI. Government Records

A. Freedom of Information Act 309
U.S. Dept. of Justice v. Reporters Committee for Freedom of Press, 489 U.S. 749 (1989) 311
National Archives and Records Administration v. Favish, 541 U.S. 157 (2004) 317

B. Fair Information Practices and the Privacy Act 322
Dinh Tran v. Department of Treasury, 351 F.Supp.3d 130 (D.D.C. 2019) 325
Doe v. Chao, 540 U.S. 614 (2004) 328
F.A.A. v. Cooper, 566 U.S. 284 (2012) 333
In re U.S. Office of Personnel Management Data Security Breach Litig., 928 F.3d 42 (D.C. Cir. 2019) 338

A. Freedom of Information Act

The federal Freedom of Information Act (FOIA) gives the public the right to request records from any federal agency. It does not apply to the courts, Congress, or state or local governments. FOIA requires each agency to publish in the Federal Register information about the kinds of records the public may obtain, how requests will be processed, and their general procedures for making information available. Agencies are only allowed to withhold information if one of the below nine exemptions applies or if the disclosure is prohibited by law. Further, if some information cannot be disclosed given those restrictions, the agency must consider whether partial disclosure is possible. Despite these apparently broad disclosure rules, those who have experienced the FOIA process tend to describe it as slow and cumbersome. FOIA disclosures are subject to the following discretionary exemptions.

> (b) [The section governing the information agencies must make available to the public] does not apply to matters that are—
>
> (1)
>
> > (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and
> >
> > (B) are in fact properly classified pursuant to such Executive order;
>
> (2) related solely to the internal personnel rules and practices of an agency;
>
> (3) specifically exempted from disclosure by statute (other than section 552b of this title), if that statute—
>
> > (A)
> >
> > > (i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or
> > >
> > > (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and
> >
> > (B) if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.
>
> (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters that would not be available by law to a party other than an agency in litigation with the agency, provided that the deliberative process privilege shall not apply to records created 25 years or more before the date on which the records were requested;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information

(A) could reasonably be expected to interfere with enforcement proceedings,

(B) would deprive a person of a right to a fair trial or an impartial adjudication,

(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,

(D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,

(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or

(F) could reasonably be expected to endanger the life or physical safety of any individual;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells.

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection. The amount of information deleted, and the exemption under which the deletion is made, shall be indicated on the released portion of the record unless including that indication would harm an interest protected by the exemption in this subsection under which the deletion is made.

The primary privacy exemptions are Exemption 6 (personnel, medical, and similar files the disclosure of which would be a "clearly unwarranted invasion of personal privacy") and Exemption 7(C) (law enforcement files the disclosure of which "could reasonably be expected to constitute an unwarranted invasion of personal privacy").

Note that these exemptions are discretionary. They do not grant individuals the affirmative right to insist that their records not be disclosed; they merely give the government the option of not disclosing. The Privacy Act (in the next section) is the main vehicle for people to insist on non-disclosure.

U.S. Dept. of Justice v. Reporters Committee for Freedom of Press, 489 U.S. 749 (1989)

Justice STEVENS delivered the opinion of the Court.

The Federal Bureau of Investigation (FBI) has accumulated and maintains criminal identification records, sometimes referred to as "rap sheets," on over 24 million persons. The question presented by this case is whether the disclosure of the contents of such a file to a third party "could reasonably be expected to constitute an unwarranted invasion of personal privacy" within the meaning of the Freedom of Information Act (FOIA).

In 1924 Congress appropriated funds to enable the Department of Justice (Department) to establish a program to collect and preserve fingerprints and other criminal identification records. That statute authorized the Department to exchange such information with "officials of States, cities and other institutions." Six years later Congress created the FBI's identification division, and gave it responsibility for "acquiring, collecting, classifying, and preserving criminal identification and other crime records and the exchanging of said criminal identification records with the duly authorized officials of governmental agencies, of States, cities, and penal institutions." Rap sheets compiled pursuant to such authority contain certain descriptive information, such as date of birth and physical characteristics, as well as a history of arrests, charges, convictions, and incarcerations of the subject. Normally a rap sheet is preserved until its subject attains age 80. Because of the volume of rap sheets, they are sometimes incorrect or incomplete and sometimes contain information about other persons with similar names.

As a matter of executive policy, the Department has generally treated rap sheets as confidential and, with certain exceptions, has restricted their use to governmental purposes. As a matter of Department policy, the FBI has made two exceptions to its general practice of prohibiting unofficial access to rap sheets. First, it allows the subject of a rap sheet to obtain a copy; and second, it occasionally allows rap sheets to be used in the preparation of press releases and publicity designed to assist in the apprehension of wanted persons or fugitives.

Although much rap-sheet information is a matter of public record, the availability and dissemination of the actual rap sheet to the public is limited. Arrests, indictments, convictions, and sentences are public events that are usually documented in court records. In addition, if a person's entire criminal history transpired in a single jurisdiction, all of the contents of his or her rap sheet may be available upon request in that jurisdiction. That possibility, however, is present in only three States. All of the other 47 States place substantial restrictions on the availability of criminal-history summaries even though individual events in those summaries are matters of public record. Moreover, even in Florida, Wisconsin, and Oklahoma, the publicly available summaries may not include information about out-of-state arrests or convictions.

The statute known as the FOIA is actually a part of the Administrative Procedure Act (APA). Section 3 of the APA as enacted in 1946 gave agencies broad discretion concerning the publication of governmental records. In 1966 Congress amended that section to implement "a general philosophy of full agency disclosure." The amendment required agencies to publish their rules of procedure in the Federal Register and to make available for public inspection and copying their opinions, statements of policy, interpretations, and staff manuals and instructions that are not published in the Federal Register. In addition, § 552(a)(3) requires every agency "upon any request for records which . . . reasonably describes such records" to make such records "promptly available to any person." If an agency improperly withholds any documents, the district court has jurisdiction to order their production. Unlike the review of other agency action that must be upheld if supported by substantial evidence and not arbitrary or capricious, the FOIA expressly places the burden "on the agency to sustain its action" and directs the district courts to "determine the matter de novo."

Congress exempted nine categories of documents from the FOIA's broad disclosure requirements. Three of those exemptions are arguably relevant to this case. Exemption 3 applies to documents that are specifically exempted from disclosure by another statute. Exemption 6 protects "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." Exemption 7(C) excludes records or information compiled for law enforcement purposes, "but only to the extent that the production of such [materials] . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy."

Exemption 7(C)'s privacy language is broader than the comparable language in Exemption 6 in two respects. First, whereas Exemption 6 requires that the invasion of privacy be "clearly unwarranted," the adverb "clearly" is omitted from Exemption 7(C). Second, whereas Exemption 6 refers to disclosures that "would constitute" an invasion of privacy, Exemption 7(C) encompasses any disclosure that "could reasonably be expected to constitute" such an invasion. Thus, the standard for evaluating a threatened invasion of privacy interests resulting from the disclosure of records compiled for law enforcement purposes is somewhat broader than the standard applicable to personnel, medical, and similar files.

This case arises out of requests made by a CBS news correspondent and the Reporters Committee for Freedom of the Press (respondents) for information concerning the criminal records of four members of the Medico family. The Pennsylvania Crime Commission had identified the family's company, Medico Industries, as a legitimate business dominated by organized crime figures. Moreover, the company allegedly had obtained a number of defense contracts as a result of an improper arrangement with a corrupt Congressman.

The FOIA requests sought disclosure of any arrests, indictments, acquittals, convictions, and sentences of any of the four Medicos. Although the FBI originally denied the requests, it provided the requested data concerning three of the Medicos after their deaths. In their complaint in the District Court, respondents sought the rap sheet for the fourth, Charles Medico (Medico), insofar as it contained "matters of public record."

The parties filed cross-motions for summary judgment. Respondents urged that any information regarding "a record of bribery, embezzlement or other financial crime" would potentially be a matter of special public interest. In answer to that argument, the Department advised respondents and the District Court that it had no record of any financial crimes concerning Medico, but the Department continued to refuse to confirm or deny whether it had any information concerning nonfinancial crimes. Thus, the issue was narrowed to Medico's nonfinancial-crime history insofar as it is a matter of public record.

Exemption 7(C) requires us to balance the privacy interest in maintaining, as the Government puts it, the "practical obscurity" of the rap sheets against the public interest in their release.

The preliminary question is whether Medico's interest in the nondisclosure of any rap sheet the FBI might have on him is the sort of "personal privacy" interest that Congress intended Exemption 7(C) to protect.[13] As we have pointed out before, "[t]he cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions." *Whalen v. Roe* (1977). Here, the former interest, "in avoiding disclosure of personal matters," is implicated.

[13] The question of the statutory meaning of privacy under the FOIA is, of course, not the same as the question whether a tort action might lie for invasion of privacy or the question whether an individual's interest in privacy is protected by the Constitution. See, *e.g., Cox Broadcasting Corp. v. Cohn* (1975) (Constitution prohibits State from penalizing publication of name of deceased rape victim obtained from public records); *Paul v. Davis* (1976) (no constitutional privacy right affected by publication of name of arrested but untried shoplifter).

Because events summarized in a rap sheet have been previously disclosed to the public, respondents contend that Medico's privacy interest in avoiding disclosure of a federal compilation of these events approaches zero. We reject respondents' cramped notion of personal privacy.

To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person. In an organized society, there are few facts that are not at one time or another divulged to another. Thus the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. According to Webster's initial definition, information may be classified as "private" if it is "intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public." Recognition of this attribute of a privacy interest supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole. The very fact that federal funds have been spent to prepare, index, and maintain these criminal-history files demonstrates that the individual items of information in the summaries would not otherwise be "freely available" either to the officials who have access to the underlying files or to the general public. Indeed, if the summaries were "freely available," there would be no reason to invoke the FOIA to obtain access to the information they contain. Granted, in many contexts the fact that information is not freely available is no reason to exempt that information from a statute generally requiring its dissemination. But the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.

This conclusion is supported by the web of federal statutory and regulatory provisions that limits the disclosure of rap-sheet information. That is, Congress has authorized rap-sheet dissemination to banks, local licensing officials, the securities industry, the nuclear-power industry, and other law enforcement agencies. Further, the FBI has permitted such disclosure to the subject of the rap sheet and, more generally, to assist in the apprehension of wanted persons or fugitives. Finally, the FBI's exchange of rap-sheet information "is subject to cancellation if dissemination is made outside the receiving departments or related agencies." This careful and limited pattern of authorized rap-sheet disclosure fits the dictionary definition of privacy as involving a restriction of information "to the use of a particular person or group or class of persons." Moreover, although perhaps not specific enough to constitute a statutory exemption under FOIA Exemption 3, these statutes and regulations, taken as a whole, evidence a congressional intent to protect the privacy of rap-sheet subjects, and a concomitant recognition of the power of compilations to affect personal privacy that outstrips the combined power of the bits of information contained within.

Also supporting our conclusion that a strong privacy interest inheres in the nondisclosure of compiled computerized information is the Privacy Act of 1974. The Privacy Act was passed largely out of concern over "the impact of computer data banks on individual privacy." The Privacy Act provides generally that "[n]o agency shall disclose any record which is contained in a system of records . . . except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." Although the Privacy Act contains a variety of exceptions to this rule, including an exemption for information required to be disclosed under the FOIA, Congress' basic policy concern regarding the implications of computerized data banks for personal privacy is certainly relevant in our consideration of the privacy interest affected by dissemination of rap sheets from the FBI computer.

Given this level of federal concern over centralized data bases, the fact that most States deny the general public access to their criminal-history summaries should not be surprising. As

we have pointed out, in 47 States nonconviction data from criminal-history summaries are not available at all, and even conviction data are "generally unavailable to the public." State policies, of course, do not determine the meaning of a federal statute, but they provide evidence that the law enforcement profession generally assumes—as has the Department of Justice—that individual subjects have a significant privacy interest in their criminal histories. It is reasonable to presume that Congress legislated with an understanding of this professional point of view.

We have also recognized the privacy interest in keeping personal facts away from the public eye. In *Whalen v. Roe* (1977), we held that "the State of New York may record, in a centralized computer file, the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs for which there is both a lawful and an unlawful market." In holding only that the Federal Constitution does not *prohibit* such a compilation, we recognized that such a centralized computer file posed a "threat to privacy":

> "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy."

In sum, the fact that "an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information." The privacy interest in a rap sheet is substantial. The substantial character of that interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80, when the FBI's rap sheets are discarded.

Exemption 7(C), by its terms, permits an agency to withhold a document only when revelation "could reasonably be expected to constitute an *unwarranted* invasion of personal privacy." We must next address what factors might *warrant* an invasion of the interest.

Our previous decisions establish that whether an invasion of privacy is *warranted* cannot turn on the purposes for which the request for information is made. Except for cases in which the objection to disclosure is based on a claim of privilege and the person requesting disclosure is the party protected by the privilege, the identity of the requesting party has no bearing on the merits of his or her FOIA request. Thus, although the subject of a presentence report can waive a privilege that might defeat a third party's access to that report, and although the FBI's policy of granting the subject of a rap sheet access to his own criminal history is consistent with its policy of denying access to all other members of the general public, the rights of the two press respondents in this case are no different from those that might be asserted by any other third party, such as a neighbor or prospective employer.

Thus whether disclosure of a private document under Exemption 7(C) is warranted must turn on the nature of the requested document and its relationship to "the basic purpose of the Freedom of Information Act 'to open agency action to the light of public scrutiny.'" *Department of Air Force v. Rose* (1976), rather than on the particular purpose for which the document is being requested. In our leading case on the FOIA, we declared that the Act was

designed to create a broad right of access to "official information." *EPA v. Mink* (1973). In his dissent in that case, Justice Douglas characterized the philosophy of the statute by quoting this comment by Henry Steele Commager:

> "The generation that made the nation thought secrecy in government one of the instruments of Old World tyranny and committed itself to the principle that a democracy cannot function unless the people are permitted to know what their government is up to."

This basic policy of "full agency disclosure unless information is exempted under clearly delineated statutory language," indeed focuses on the citizens' right to be informed about "what their government is up to." Official information that sheds light on an agency's performance of its statutory duties falls squarely within that statutory purpose. That purpose, however, is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency's own conduct. In this case—and presumably in the typical case in which one private citizen is seeking information about another—the requester does not intend to discover anything about the conduct of the agency that has possession of the requested records. Indeed, response to this request would not shed any light on the conduct of any Government agency or official.

Respondents argue that there is a two-fold public interest in learning about Medico's past arrests or convictions: He allegedly had improper dealings with a corrupt Congressman, and he is an officer of a corporation with defense contracts. But if Medico has, in fact, been arrested or convicted of certain crimes, that information would neither aggravate nor mitigate his allegedly improper relationship with the Congressman; more specifically, it would tell us nothing directly about the character of the *Congressman's* behavior. Nor would it tell us anything about the conduct of the *Department of Defense* (DOD) in awarding one or more contracts to the Medico Company. Arguably a FOIA request to the DOD for records relating to those contracts, or for documents describing the agency's procedures, if any, for determining whether officers of a prospective contractor have criminal records, would constitute an appropriate request for "official information." Conceivably Medico's rap sheet would provide details to include in a news story, but, in itself, this is not the kind of public interest for which Congress enacted the FOIA. In other words, although there is undoubtedly some public interest in anyone's criminal history, especially if the history is in some way related to the subject's dealing with a public official or agency, the FOIA's central purpose is to ensure that the *Government's* activities be opened to the sharp eye of public scrutiny, not that information about *private citizens* that happens to be in the warehouse of the Government be so disclosed. Thus, it should come as no surprise that in none of our cases construing the FOIA have we found it appropriate to order a Government agency to honor a FOIA request for information about a particular private citizen.

What we have said should make clear that the public interest in the release of any rap sheet on Medico that may exist is not the type of interest protected by the FOIA. Medico may or may not be one of the 24 million persons for whom the FBI has a rap sheet. If respondents are entitled to have the FBI tell them what it knows about Medico's criminal history, any other member of the public is entitled to the same disclosure—whether for writing a news story, for deciding whether to employ Medico, to rent a house to him, to extend credit to him, or simply to confirm or deny a suspicion. There is, unquestionably, *some* public interest in providing interested citizens with answers to their questions about Medico. But that interest falls outside the ambit of the public interest that the FOIA was enacted to serve.

The Court of Appeals majority expressed concern about assigning federal judges the task of striking a proper case-by-case, or ad hoc, balance between individual privacy interests and the public interest in the disclosure of criminal-history information without providing those judges standards to assist in performing that task. Our cases provide support for the proposition

that categorical decisions may be appropriate and individual circumstances disregarded when a case fits into a genus in which the balance characteristically tips in one direction.

The privacy interest in maintaining the practical obscurity of rap-sheet information will always be high. When the subject of such a rap sheet is a private citizen and when the information is in the Government's control as a compilation, rather than as a record of "what the Government is up to," the privacy interest protected by Exemption 7(C) is in fact at its apex while the FOIA-based public interest in disclosure is at its nadir. Such a disparity on the scales of justice holds for a class of cases without regard to individual circumstances; the standard virtues of bright-line rules are thus present, and the difficulties attendant to ad hoc adjudication may be avoided. Accordingly, we hold as a categorical matter that a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that when the request seeks no "official information" about a Government agency, but merely records that the Government happens to be storing, the invasion of privacy is "unwarranted." The judgment of the Court of Appeals is reversed.

Justice BLACKMUN, with whom Justice BRENNAN joins, concurring in the judgment.

I concur in the result the Court reaches in this case, but I cannot follow the route the Court takes to reach that result. In other words, the Court's use of "categorical balancing" under Exemption 7(C), I think, is not basically sound. Such a bright-line rule obviously has its appeal, but I wonder whether it would not run aground on occasion, such as in a situation where a rap sheet discloses a congressional candidate's conviction of tax fraud five years before. Surely, the FBI's disclosure of that information could not "reasonably be expected" to constitute an invasion of personal privacy, much less an unwarranted invasion, inasmuch as the candidate relinquished any interest in preventing the dissemination of this information when he chose to run for Congress.

For these reasons, I would not adopt the Court's bright-line approach but would leave the door open for the disclosure of rap-sheet information in some circumstances. Nonetheless, even a more flexible balancing approach would still require reversing the Court of Appeals in this case. I, therefore, concur in the judgment, but do not join the Court's opinion.

Notes

1. Alert readers may note that this case, protecting the rap-sheet privacy of suspected criminals, came the same year as *Florida Star*, which failed to protect the privacy of rape victims whose names were disclosed in government documents. The dissent in *Florida Star* did not fail to appreciate the contrast:

> Ironically, this Court, too, had occasion to consider this same balance just a few weeks ago, in *United States Department of Justice v. Reporters Committee for Freedom of Press* (1989). There, we were faced with a press request, under the Freedom of Information Act, for a "rap sheet" on a person accused of bribing a Congressman—presumably, a person whose privacy rights would be far less than B.J.F.'s. Yet this Court rejected the media's request for disclosure of the "rap sheet," saying:
>
> "The privacy interest in maintaining the practical obscurity of rap-sheet information will always be high. When the subject of such a rap sheet is a private citizen and when the information is in the Government's control as a compilation, rather than as a record of 'what the government is up to,' the privacy interest . . . is . . . at its apex while the . . . public interest in disclosure is at its nadir."

> The Court went on to conclude that disclosure of rap sheets "categorical[ly]" constitutes an "unwarranted" invasion of privacy. The same surely must be true—indeed, much more so—for the disclosure of a rape victim's name.

2. Not all law enforcement information is exempt from FOIA disclosure. The D.C. Circuit held that a categorical assertion of Exemption 7(C) was untenable when a public interest organization requested law enforcement files related to an investigation of corrupt lobbyist Jack Abramoff and his dealings with former House Majority Leader Tom DeLay. "Information about the FBI's and the DOJ's investigation of major, wide-ranging public corruption is more likely to shed light on how the agencies are performing their statutory duties than a discrete internal disciplinary proceeding. Although a substantial privacy interest is at stake here, in light of the similarly substantial countervailing public interest, the balance does not characteristically tip in favor of non-disclosure." *Citizens for Resp. & Ethics in Wash. v. U.S. Dep't of Just.*, 746 F.3d 1082, 1096 (D.C. Cir. 2014).
3. In a footnote, the Court wrote that FOIA might protect the privacy of information that was not protected by the constitutional right to privacy. Notably, courts have had little trouble permitting the government to voluntarily disclose exactly the type of information that the FOIA exemptions protect. For example, the Supreme Court held in *Paul v. Davis*, 424 U.S. 693 (1976) that Davis, who had been arrested but not yet convicted of shoplifting, had no constitutional protection against the government for distributing a flyer naming him an "active shoplifter." Specifically, the court contrasted Davis's claim with those that had been successful in the then-developing constitutional privacy space:

> The activities detailed as being within this definition were ones very different from that for which respondent claims constitutional protection -- matters relating to marriage, procreation, contraception, family relationships, and childrearing and education. In these areas, it has been held that there are limitations on the States' power to substantively regulate conduct.
>
> Respondent's claim is far afield from this line of decisions. He claims constitutional protection against the disclosure of the fact of his arrest on a shoplifting charge. His claim is based, not upon any challenge to the State's ability to restrict his freedom of action in a sphere contended to be "private," but instead on a claim that the State may not publicize a record of an official act such as an arrest.

This case predates *Whalen v. Roe* and some of the other constitutional privacy cases, but even decades later circuit courts held that there is "no privacy interest in one's criminal record that is protected by the United States Constitution." *Cline v. Rogers,* 87 F.3d 176 (6th Cir. 1996) (holding that there is no constitutional or statutory issue with a police department releasing both state and federal criminal history information to a private citizen).

National Archives and Records Administration v. Favish, 541 U.S. 157 (2004)

Justice KENNEDY delivered the opinion of the Court.

This case requires us to interpret the Freedom of Information Act (FOIA). FOIA does not apply if the requested data fall within one or more exemptions. Exemption 7(C) excuses from disclosure "records or information compiled for law enforcement purposes" if their production "could reasonably be expected to constitute an unwarranted invasion of personal privacy."

In *Department of Justice v. Reporters Comm. for Freedom of Press* (1989), we considered the scope of Exemption 7(C) and held that release of the document at issue would be a prohibited invasion of the personal privacy of the person to whom the document referred. The principal

document involved was the criminal record, or rap sheet, of the person who himself objected to the disclosure. Here, the information pertains to an official investigation into the circumstances surrounding an apparent suicide. The initial question is whether the exemption extends to the decedent's family when the family objects to the release of photographs showing the condition of the body at the scene of death. If we find the decedent's family does have a personal privacy interest recognized by the statute, we must then consider whether that privacy claim is outweighed by the public interest in disclosure.

Vincent Foster, Jr., deputy counsel to President Clinton, was found dead in Fort Marcy Park, located just outside Washington, D.C. The United States Park Police conducted the initial investigation and took color photographs of the death scene, including 10 pictures of Foster's body. The investigation concluded that Foster committed suicide by shooting himself with a revolver. Subsequent investigations by the Federal Bureau of Investigation, committees of the Senate and the House of Representatives, and independent counsels Robert Fiske and Kenneth Starr reached the same conclusion. Despite the unanimous finding of these five investigations, a citizen interested in the matter, Allan Favish, remained skeptical. Favish is now a respondent in this proceeding. In an earlier proceeding, Favish was the associate counsel for Accuracy in Media (AIM), which applied under FOIA for Foster's death-scene photographs. After the National Park Service, which then maintained custody of the pictures, resisted disclosure, Favish filed suit on behalf of AIM in the District Court for the District of Columbia to compel production. The District Court granted summary judgment against AIM. The Court of Appeals for the District of Columbia unanimously affirmed.

Still convinced that the Government's investigations were "grossly incomplete and untrustworthy," Favish filed the present FOIA request in his own name, seeking, among other things, 11 pictures, 1 showing Foster's eyeglasses and 10 depicting various parts of Foster's body. Like the National Park Service, the Office of Independent Counsel (OIC) refused the request under Exemption 7(C).

It is common ground among the parties that the death-scene photographs in OIC's possession are records or information "compiled for law enforcement purposes" as that phrase is used in Exemption 7(C). This leads to the question whether disclosure . . . "could reasonably be expected to constitute an unwarranted invasion of personal privacy."

Favish contends the family has no personal privacy interest covered by Exemption 7(C). His argument rests on the proposition that the information is only about the decedent, not his family. FOIA's right to personal privacy, in his view, means only "the right to control information about oneself." He quotes from our decision in *Reporters Committee,* where, in holding that a person has a privacy interest sufficient to prevent disclosure of his own rap sheet, we said "the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." This means, Favish says, that the individual who is the subject of the information is the only one with a privacy interest.

We disagree. Favish misreads the quoted sentence in *Reporters Committee* and adopts too narrow an interpretation of the case's holding. To say that the concept of personal privacy must "encompass" the individual's control of information about himself does not mean it cannot encompass other personal privacy interests as well. *Reporters Committee* had no occasion to consider whether individuals whose personal data are not contained in the requested materials also have a recognized privacy interest under Exemption 7(C).

Reporters Committee explained, however, that the concept of personal privacy under Exemption 7(C) is not some limited or "cramped notion" of that idea. Records or information are not to be released under FOIA if disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy." This provision is in marked contrast to the language in Exemption 6, pertaining to "personnel and medical files," where withholding is required only if disclosure "would constitute a clearly unwarranted invasion of personal privacy." The adverb

"clearly," found in Exemption 6, is not used in Exemption 7(C). In addition, "whereas Exemption 6 refers to disclosures that 'would constitute' an invasion of privacy, Exemption 7(C) encompasses any disclosure that 'could reasonably be expected to constitute' such an invasion." *Reporters Committee*.

Law enforcement documents obtained by Government investigators often contain information about persons interviewed as witnesses or initial suspects but whose link to the official inquiry may be the result of mere happenstance. There is special reason, therefore, to give protection to this intimate personal data, to which the public does not have a general right of access in the ordinary course. In this class of cases where the subject of the documents "is a private citizen," "the privacy interest . . . is at its apex."

Certain *amici* in support of Favish rely on the modifier "personal" before the word "privacy" to bolster their view that the family has no privacy interest in the pictures of the decedent. This, too, misapprehends the family's position and the scope of protection the exemption provides. The family does not invoke Exemption 7(C) on behalf of Vincent Foster in its capacity as his next friend for fear that the pictures may reveal private information about Foster to the detriment of his own posthumous reputation or some other interest personal to him. If that were the case, a different set of considerations would control. Foster's relatives instead invoke their own right and interest to personal privacy. They seek to be shielded by the exemption to secure their own refuge from a sensation-seeking culture for their own peace of mind and tranquility, not for the sake of the deceased.

In a sworn declaration filed with the District Court, Foster's sister, Sheila Foster Anthony, stated that the family had been harassed by, and deluged with requests from, "[p]olitical and commercial opportunists" who sought to profit from Foster's suicide. In particular, she was "horrified and devastated by [a] photograph [already] leaked to the press." "[E]very time I see it," Sheila Foster Anthony wrote, "I have nightmares and heart-pounding insomnia as I visualize how he must have spent his last few minutes and seconds of his life." She opposed the disclosure of the disputed pictures because "I fear that the release of [additional] photographs certainly would set off another round of intense scrutiny by the media. Undoubtedly, the photographs would be placed on the Internet for world consumption. Once again my family would be the focus of conceivably unsavory and distasteful media coverage." "[R]eleasing any photographs," Sheila Foster Anthony continued, "would constitute a painful unwarranted invasion of my privacy, my mother's privacy, my sister's privacy, and the privacy of Lisa Foster Moody (Vince's widow), her three children, and other members of the Foster family."

As we shall explain below, we think it proper to conclude from Congress' use of the term "personal privacy" that it intended to permit family members to assert their own privacy rights against public intrusions long deemed impermissible under the common law and in our cultural traditions. This does not mean that the family is in the same position as the individual who is the subject of the disclosure. We have little difficulty, however, in finding in our case law and traditions the right of family members to direct and control disposition of the body of the deceased and to limit attempts to exploit pictures of the deceased family member's remains for public purposes.

Burial rites or their counterparts have been respected in almost all civilizations from time immemorial. See generally 26 Encyclopaedia Britannica 851 (15th ed.1985) (noting that "[t]he ritual burial of the dead" has been practiced "from the very dawn of human culture and . . . in most parts of the world"); 5 Encyclopedia of Religion 450 (1987) ("[F]uneral rites . . . are the conscious cultural forms of one of our most ancient, universal, and unconscious impulses"). They are a sign of the respect a society shows for the deceased and for the surviving family members. The power of Sophocles' story in Antigone maintains its hold to this day because of the universal acceptance of the heroine's right to insist on respect for the body of her brother. The outrage at seeing the bodies of American soldiers mutilated and dragged through the

streets is but a modern instance of the same understanding of the interests decent people have for those whom they have lost. Family members have a personal stake in honoring and mourning their dead and objecting to unwarranted public exploitation that, by intruding upon their own grief, tends to degrade the rites and respect they seek to accord to the deceased person who was once their own.

In addition this well-established cultural tradition acknowledging a family's control over the body and death images of the deceased has long been recognized at common law. Indeed, this right to privacy has much deeper roots in the common law than the rap sheets held to be protected from disclosure in *Reporters Committee.* An early decision by the New York Court of Appeals is typical:

> "It is the right of privacy of the living which it is sought to enforce here. That right may in some cases be itself violated by improperly interfering with the character or memory of a deceased relative, but it is the right of the living, and not that of the dead, which is recognized. A privilege may be given the surviving relatives of a deceased person to protect his memory, but the privilege exists for the benefit of the living, to protect their feelings, and to prevent a violation of their own rights in the character and memory of the deceased." *Schuyler v. Curtis* (1895).

We can assume Congress legislated against this background of law, scholarship, and history when it enacted FOIA and when it amended Exemption 7(C) to extend its terms.

We have observed that the statutory privacy right protected by Exemption 7(C) goes beyond the common law and the Constitution. It would be anomalous to hold in the instant case that the statute provides even less protection than does the common law.

The statutory scheme must be understood, moreover, in light of the consequences that would follow were we to adopt Favish's position. As a general rule, withholding information under FOIA cannot be predicated on the identity of the requester. We are advised by the Government that child molesters, rapists, murderers, and other violent criminals often make FOIA requests for autopsies, photographs, and records of their deceased victims. Our holding ensures that the privacy interests of surviving family members would allow the Government to deny these gruesome requests in appropriate cases. We find it inconceivable that Congress could have intended a definition of "personal privacy" so narrow that it would allow convicted felons to obtain these materials without limitations at the expense of surviving family members' personal privacy.

For these reasons . . . we hold that FOIA recognizes surviving family members' right to personal privacy with respect to their close relative's death-scene images. Our holding is consistent with the unanimous view of the Courts of Appeals and other lower courts that have addressed the question. Neither the deceased's former status as a public official, nor the fact that other pictures had been made public, detracts from the weighty privacy interests involved.

Our ruling that the personal privacy protected by Exemption 7(C) extends to family members who object to the disclosure of graphic details surrounding their relative's death does not end the case. Although this privacy interest is within the terms of the exemption, the statute directs nondisclosure only where the information "could reasonably be expected to constitute an unwarranted invasion" of the family's personal privacy. The term "unwarranted" requires us to balance the family's privacy interest against the public interest in disclosure.

FOIA is often explained as a means for citizens to know "what their Government is up to." This phrase should not be dismissed as a convenient formalism. It defines a structural necessity in a real democracy. The statement confirms that, as a general rule, when documents are within FOIA's disclosure provisions, citizens should not be required to explain why they seek the information. A person requesting the information needs no preconceived idea of the

uses the data might serve. The information belongs to citizens to do with as they choose. Furthermore, as we have noted, the disclosure does not depend on the identity of the requester. As a general rule, if the information is subject to disclosure, it belongs to all.

When disclosure touches upon certain areas defined in the exemptions, however, the statute recognizes limitations that compete with the general interest in disclosure, and that, in appropriate cases, can overcome it. In the case of Exemption 7(C), the statute requires us to protect, in the proper degree, the personal privacy of citizens against the uncontrolled release of information compiled through the power of the State. The statutory direction that the information not be released if the invasion of personal privacy could reasonably be expected to be unwarranted requires the courts to balance the competing interests in privacy and disclosure. To effect this balance and to give practical meaning to the exemption, the usual rule that the citizen need not offer a reason for requesting the information must be inapplicable.

Where the privacy concerns addressed by Exemption 7(C) are present, the exemption requires the person requesting the information to establish a sufficient reason for the disclosure. First, the citizen must show that the public interest sought to be advanced is a significant one, an interest more specific than having the information for its own sake. Second, the citizen must show the information is likely to advance that interest. Otherwise, the invasion of privacy is unwarranted.

We do not in this single decision attempt to define the reasons that will suffice, or the necessary nexus between the requested information and the asserted public interest that would be advanced by disclosure. On the other hand, there must be some stability with respect to both the specific category of personal privacy interests protected by the statute and the specific category of public interests that could outweigh the privacy claim. Otherwise, courts will be left to balance in an ad hoc manner with little or no real guidance. In the case of photographic images and other data pertaining to an individual who died under mysterious circumstances, the justification most likely to satisfy Exemption 7(C)'s public interest requirement is that the information is necessary to show the investigative agency or other responsible officials acted negligently or otherwise improperly in the performance of their duties.

We hold that, where there is a privacy interest protected by Exemption 7(C) and the public interest being asserted is to show that responsible officials acted negligently or otherwise improperly in the performance of their duties, the requester must establish more than a bare suspicion in order to obtain disclosure. Rather, the requester must produce evidence that would warrant a belief by a reasonable person that the alleged Government impropriety might have occurred. In *Department of State v. Ray* (1991), we held there is a presumption of legitimacy accorded to the Government's official conduct. The presumption perhaps is less a rule of evidence than a general working principle. However the rule is characterized, where the presumption is applicable, clear evidence is usually required to displace it. Given FOIA's prodisclosure purpose, however, the less stringent standard we adopt today is more faithful to the statutory scheme. Only when the FOIA requester has produced evidence sufficient to satisfy this standard will there exist a counterweight on the FOIA scale for the court to balance against the cognizable privacy interests in the requested records. Allegations of government misconduct are “easy to allege and hard to disprove,” *Crawford–El v. Britton* (1998), so courts must insist on a meaningful evidentiary showing. It would be quite extraordinary to say we must ignore the fact that five different inquiries into the Foster matter reached the same conclusion. As we have noted, the balancing exercise in some other case might require us to make a somewhat more precise determination regarding the significance of the public interest and the historical importance of the events in question. We might need to consider the nexus required between the requested documents and the purported public interest served by disclosure. We need not do so here, however. Favish has not produced any evidence that would warrant a belief by a reasonable person that the alleged Government impropriety might have occurred to put the balance into play.

Notes

1. It is difficult to convey the fever swamp of right-wing conspiracy theories that surrounded the death of Vince Foster. Two basic facts may help contextualize it. First, it is not normal for there to be five separate investigations into the same death, especially when each returns a conclusion of suicide. Second, I was having lunch with a pair of distinguished older gentlemen and one of them confided in me that he still thought that Vince Foster did not kill himself. The matter had apparently been occupying his thoughts. The lunch occurred in 2016; Foster's death occurred in 1993.
2. Under the *Favish* test, the strength of a requester's justifications is relevant "where the privacy concerns addressed by Exemption 7(C) are present." Lior Strahilevitz argues that this is unsatisfying. Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CAL. L. REV. 2007, 2024 (2010). If there is no government misconduct in investigations 1, 2, 3, and 4, then investigation 5 is likely a waste of government resources. He posits that a person seeking the same photos to show that the continual reinvestigations were wasteful and politically motivated misconduct should be allowed to obtain them under the *Favish* test, making the analysis easily manipulated.

B. Fair Information Practices and the Privacy Act

Rooted in a 1973 U.S. Department of Health, Education, and Welfare Advisory Committee report, the Fair Information Practice Principles have shaped both American and international privacy law. The report was the first comprehensive study of privacy risks arising from the federal government's shift from paper records to electronic systems for creating, storing, and retrieving information. Traces of the Fair Information Practices are present in almost every privacy law covered in this book, such as HIPAA, the Fair Credit Reporting Act, and the California Consumer Privacy Act. Despite the influence of these principles across different pieces of legislation and regulation, however, their lofty objectives are rarely realized in full.

> *Access and Amendment*. Agencies should provide individuals with appropriate access to personally identifiable information (PII) and appropriate opportunity to correct or amend PII.
>
> *Accountability*. Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.
>
> *Authority*. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.
>
> *Minimization*. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.
>
> *Quality and Integrity*. Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

Individual Participation. Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

Purpose Specification and Use Limitation. Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

Security. Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

Transparency. Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

The relevance of these principles to different data systems may vary. For instance, a right to correction is far more important in the context of consumer credit reports—where an error may lead to the loss of a job— than in the context of targeted advertising. Data security, in contrast, is relevant in almost any data system.

The Fair Information Practices were finalized in 1973. In 1974, Congress drew heavily on them when it passed the Privacy Act, which governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

The Privacy Act requires that agencies give the public notice of their systems of records by publishing in the Federal Register. It also prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual unless the disclosure is pursuant to one of twelve statutory exceptions. In addition to this protection against disclosure, people can also seek access to and amendment of their records.

Scope. The Privacy Act—like FOIA—applies only to federal Executive Branch agencies, and it incorporates FOIA's definition of "agency." The White House, federal courts, and entities merely linked to the federal government are not "agencies," nor are state governments or their departments. Though the Act applies to government corporations and government-controlled corporations, it does not apply to private companies even if those companies hold government contracts.

The Act gives rights to individuals. Under the Act, "the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence." 5 U.S.C. § 552a(a)(2).

The Act governs "records" in a "system of records." "[T]he term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4).

"[T]he term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying

number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).

An example of such a record in a system of records would be a person's tax return, security clearance form, or application for social security benefits. These are all records that are about an individual, indexed by their name, and stored within an organized record system. The private notes a government representative took after meeting with an individual would not be such a record. Nor would forwarded emails, office gossip, or a wide variety of other unorganized data.

Protections. The Privacy Act sets out a broad "no disclosure without consent" rule. "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains [subject to twelve exceptions]." 5 U.S.C. § 552a(b). Federal guidelines caution that "the consent provision was not intended to permit a blanket or open-ended consent clause, i.e., one which would permit the agency to disclose a record without limit," and that, "[a]t a minimum, the consent clause should state the general purposes for, or types of recipients [to] which disclosure may be made."[143]

The twelve exceptions permit substantial internal government use of records, however. Though many of the below are quite limited and specific (4, 5, 6), several are broad (particularly 1, 2, and 3). 5 U.S.C. § 552a(b)

> (1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
>
> (2) required under section 552 of this title [the Freedom of Information Act];
>
> (3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section [see below];
>
> (4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity…;
>
> (5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
>
> (6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;
>
> (7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
>
> (8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

---

[143] Privacy Act Guidelines, Vol. 40, No. 132 FEDERAL REGISTER 28949, 28954 (1975) https://www.justice.gov/d9/pages/attachments/2021/02/24/omb_1975_guidelines_0.pdf

> (9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
>
> (10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the Government Accountability Office;
>
> (11) pursuant to the order of a court of competent jurisdiction; or
>
> (12) to a consumer reporting agency in accordance with section 3711(e) of title 31 [about outstanding financial collections].

The most important of these exceptions are numbers 1, 2, and 3. Exception 1 permits disclosures internal to the agency when the receiver needs to know the information to perform their duties. So, there is no issue under the Privacy Act with one employee of the IRS sharing a tax return with another, provided that the receiver has a legitimate need to see it. Nor are there issues with sharing internal employee records to aid employee misconduct investigations.

Exception 2 covers releases required by FOIA. Consider how FOIA works. Information must be released if it is properly requested unless it falls within the scope of a discretionary exemption. So, if information release is required by FOIA, the release of that information does not raise an issue under the Privacy Act. If a FOIA exemption applies, however, FOIA does not *require* the release. This means that the government's failure to assert a FOIA exemption can lead to liability under the Privacy Act.

Exception 3 covers "routine uses." This is a defined term under the Act. A routine use is a disclosure for a "purpose which is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(a)(7). This exception is broad, but agencies must publish in the Federal Register a list of their routine uses of records.

To understand how the "routine use" and "need-to-know" exceptions apply in practice, consider the following case about government employee records.

Dinh Tran v. Department of Treasury, 351 F.Supp.3d 130 (D.D.C. 2019)

TREVOR N. McFADDEN, U.S.D.J.

Plaintiff Dinh Tran, a former employee of the U.S. Department of the Treasury, alleges that it disclosed her annual performance appraisal in violation of the Privacy Act, 5 U.S.C. § 552a. The Treasury admits that it disclosed Ms. Tran's performance appraisal, a protected record. But the Treasury argues that the Privacy Act's "routine use" exception and "need-to-know" exception permit the disclosure. So the Treasury has moved for summary judgment. The "routine use" exception does not apply, but the Treasury's motion will be granted because the "need-to-know" exception applies.

Dinh Tran was an Attorney-Advisory in the Office of Professional Responsibility ("OPR") within the Internal Revenue Service ("IRS"). She applied for a six-month detail with the Washington, D.C., field office of Division Counsel, Small Business/Self-Employed ("SB/SE"). SB/SE is within the Office of the Chief Counsel ("OCC") for the IRS, and it provides legal advice to various components within the Treasury.

When considering an employee-initiated detail request from an IRS employee, SB/SE's practice is to evaluate the requesting employee's knowledge, skills, and experience to determine whether the detail would benefit SB/SE and the requesting employee. SB/SE therefore requests the employee's resume and most recent performance appraisal.

[The performance appraisal was shared, Tran was interviewed, and the front-line managers recommended against approving the request. She then accepted a detail to another division.]

Ms. Tran sued, alleging that disclosure of her performance appraisal violated the Privacy Act, 5 U.S.C. § 552a. The Treasury concedes that the Privacy Act protects employees' performance appraisals, the Treasury disclosed the record, and it did not get Ms. Tran's consent beforehand. But the Treasury argues that the disclosure was permissible under the Privacy Act's "routine use" exception and its "need-to-know" exception. The Treasury thus moves for summary judgment.

The parties agree that Ms. Tran did not consent to the Treasury disclosing her performance appraisal. But disclosure is also proper where any of twelve enumerated exceptions applies.

Section 552a(b)(3) allows agencies to disclose otherwise protected records "for a routine use as defined in subsection (a)(7)." A "routine use," for the disclosure of a record, is the use of a record "for a purpose which is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(a)(7). Agencies must publish in the Federal Register "each routine use of the records contained in the system, including the categories of users and the purpose of such use." These regulations are known as Systems of Records Notice (SORNs).

The Treasury maintains that SORN 36.003, *General Personnel and Payroll Records*, covers the disclosure here. This SORN applies to current and former employees of the Treasury and covers records, like Ms. Tran's performance appraisal, in the employee's Employee Performance File. The Treasury first points to SORN 36.003(3), which allows it to

> [d]isclose information to a Federal, state, local, or tribal agency, or other public authority, which has requested information relevant or necessary to hiring or retaining an employee, or issuing or continuing a contract, security clearance, license, grant, or other benefit.

Next, the Treasury points to SORN 36.003(9), which allows it to "[d]isclose information to a prospective employer of an IRS employee or former IRS employee."

According to the Treasury, it was a "prospective employer" of Ms. Tran and her detail request was a hiring action. Thus, it argues that either SORN 36.003(3) or 36.003(9) covers the disclosure of Ms. Tran's performance appraisal. But the Treasury has not shown that it was a "prospective employer" or that Ms. Tran's detail was a "hiring" action.

The problem with the Treasury's theory is that when Ms. Tran requested a detail, the Treasury was already her employer. As discussed, Ms. Tran was an attorney with OPR, a Treasury component. The Treasury has not shown how it may qualify simultaneously as a current employer and a "prospective employer" under SORN 36.003(9), and it has cited no caselaw to support its position. Just as a hungry child may not have his cake and eat it too, so an agency may not employ someone and also be her prospective employer.

Nor has the Treasury showed that a detail is a hiring action under SORN 36.003(3). As Ms. Tran points out, federal statutes and regulations that authorize executive agencies to hire non-employees are distinct from those that authorize agencies to detail current employees to different offices within the agency. When an agency details an employee, it has already hired her; the employee is merely being assigned temporarily to a different position within the employing organization.

Next, the Treasury argues that the "routine use" exception applies because SORN 36.003(3) permits the agency to disclose "information to a Federal . . . public authority, which has requested information relevant or necessary to . . . issuing or continuing a . . . benefit." But when an agency publishes the routine uses for a record, it must include "the purposes of such use," 5 U.S.C. § 552a(3)(4)(D), and the broad term "benefit" does not provide adequate notice of

the purposes for which the Treasury may release an employee's information. *Britt v. Naval Invest. Serv.* (3d Cir. 1989).[7]

The Treasury's next argument is on the money. Section 552a(b)(1) is known as the intra-agency "need-to-know" exception. It permits agencies to disclose otherwise protected records "to officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." The Treasury correctly contends that this section permits the disclosure of Ms. Tran's performance appraisal.

First, the disclosure here was "intra-agency," because both OPR and SB/SE are Treasury components. Ms. Tran does not argue otherwise. And other courts that have considered Privacy Act claims involving disclosures between separate offices within a department have evaluated claims from the Executive Department-level perspective.

Second, the Treasury employees who examined Ms. Tran's performance appraisal had a "need-to-know" the information. "What matters . . . is the 'need-to-know' of the agency official who *received* the disclosure . . . ." And "[s]ection 552a(b)(1) does not require an agency to list those of its officers eligible to look at protected records, nor does it demand that an agency official be specifically assigned to examining records." Instead, the Court should determine "whether the official examined the record in connection with the performance of duties assigned to him and whether he had to do so to perform those duties properly." In other words, did the examining official have a legitimate purpose for the review, or was he improperly accessing an employee's private records?

Here, the disclosure of Ms. Tran's performance appraisal to Ms. Romano, Mr. Rath, and the front-line managers in the D.C. field office falls comfortably within § 552a(b)(1). Remember that Ms. Tran began this disclosure—although perhaps unwittingly—by applying for a detail in this office. Mr. Meneely then tasked the Area Counsel and front-line managers with evaluating Ms. Tran's detail request and recommending whether to approve it. As he explained, "[t]hey're the people that have to train and manage any potential detailee." The only time that these individuals examined Ms. Tran's performance appraisal was in performing their assigned duty.

And they had a need-to-know the information in Ms. Tran's performance appraisal to perform their assigned duty properly. Agencies often invoke the "need-to-know" exception when they release records for a disciplinary investigation. But it equally applies to a detail decision. Both are decisions about whether an employee is fit for a position within the agency or can perform certain duties. Both are triggered by the employee's actions, not supervisory caprice.

The Privacy Act certainly does not require agencies to make uninformed personnel decisions. Indeed, courts have recognized that "[t]he 'need-to-know' exception permits the disclosure of a person's protected record to a supervisor who needs the information contained in the record to assess the person's trustworthiness and make related personnel decision." And the front-line managers recommended against approving Ms. Tran's detail request in part because "they did not believe that Ms. Tran had the litigation skillset needed to be a docket attorney in the D.C. field office."

But Ms. Tran complains that Mr. Meneely, who supervises the Area Counsel and front-line managers just discussed, did not need to view her performance appraisal to perform his duties. Not so. Of course, "the need-to-know exception is not limited only to officers and

---

[7] In *Britt*, the court noted that purpose of the publication requirement was to provide "meaningful public notice," and "[i]t was Congress' intent that the routine use exception should serve as a caution to agencies to think in advance what uses [they] will make of the information." *[S]ee also Radack v. Dep't of Justice* (D.D.C. 2005) ("In order to ensure that people are aware of the purpose for which their information might be disclosed, agencies are required to publish each routine use in the Federal Register.").

employees within a certain office within an agency rather than to officers and employees of the entire agency." In *Hanna v. Herman* (D.D.C. 2000), the court found that an agency supervisor's disclosure of information about the plaintiff's demotion to a supervisor elsewhere in the agency "would be covered by the 'need-to-know' exception as a matter of law."

As Deputy Division Counsel responsible for SB/SE's field operations, including for the D.C. field office, Mr. Meneely was among the highest-ranking officials in SB/SE Division Counsel's office. Courts have recognized that the "need-to-know" exception "encompasses personnel matters," and Mr. Meneely would have needed to know the information disclosed about Ms. Tran because of his supervisory role in determining her suitability for a detail in his office.

Notes

1. This painfully nitpicky analysis of the Federal Register is typical in Privacy Act "routine use" cases. The district court in the below *F.A.A. v. Cooper* case performs a similar analysis. Does this make sense? What is the virtue of making federal agencies file these detailed disclosures in the Federal Register? Presumably almost no one actually reads them.
   The best defense of this practice is that the publication requirement forces a slight level of transparency and preplanning. The agency itself is forced to think ahead about how it would like to use and share data. It is then forced to put that plan in a public document that lawyers and advocacy groups have the opportunity to read. If the agency is contemplating a truly new data sharing regime, the publication requirement slows the process.
2. The "routine use" exception has been referred to as the Privacy Act's biggest loophole. In practice, an agency will often have the ability to 1) define the purpose for which information was initially collected broadly enough to encompass many subsequent uses, and 2) publish in the Federal Register a broad enough description of what it would like to do with the information that it will have given effective notice of the subsequent uses. Nevertheless, plaintiffs do win on these points sometimes due to the level of precision required by courts.

Doe v. Chao, 540 U.S. 614 (2004)

Justice SOUTER delivered the opinion of the Court.

The United States is subject to a cause of action for the benefit of at least some individuals adversely affected by a federal agency's violation of the Privacy Act of 1974. The question before us is whether plaintiffs must prove some actual damages to qualify for a minimum statutory award of $1,000. We hold that they must.

Petitioner Buck Doe filed for benefits under the Black Lung Benefits Act, 83 Stat. 792, 30 U.S.C. § 901 *et seq.,* with the Office of Workers' Compensation Programs, the division of the Department of Labor responsible for adjudicating it. The application form called for a Social Security number, which the agency then used to identify the applicant's claim, as on documents like "multicaptioned" notices of hearing dates, sent to groups of claimants, their employers, and the lawyers involved in their cases. The Government concedes that following this practice led to disclosing Doe's Social Security number beyond the limits set by the Privacy Act. See 5 U.S.C. § 552a(b).

Doe joined with six other black lung claimants to sue the Department of Labor, alleging repeated violations of the Act and seeking certification of a class of "all claimants for Black Lung Benefits since the passage of the Privacy Act." Early on, the United States stipulated to an order prohibiting future publication of applicants' Social Security numbers on multicaptioned hearing notices, and the parties then filed cross-motions for summary judgment. The District Court denied class certification and entered judgment against all individual plaintiffs except Doe, finding that their submissions had raised no issues of cognizable harm. As to Doe, the court accepted his uncontroverted evidence of distress on learning of the improper

disclosure, granted summary judgment, and awarded $1,000 in statutory damages under 5 U.S.C. § 552a(g)(4).

A divided panel of the Fourth Circuit affirmed in part but reversed on Doe's claim, holding the United States entitled to summary judgment across the board. We now affirm.

"[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.

Subsection (g)(1) recognizes a civil action for agency misconduct fitting within any of four categories (the fourth, in issue here, being a catchall), 5 U.S.C. §§ 552a(g)(1)(A)–(D), and then makes separate provision for the redress of each. The first two categories cover deficient management of records: subsection (g)(1)(A) provides for the correction of any inaccurate or otherwise improper material in a record, and subsection (g)(1)(B) provides a right of access against any agency refusing to allow an individual to inspect a record kept on him.

The two remaining categories deal with derelictions having consequences beyond the statutory violations *per se*. Subsection (g)(1)(C) describes an agency's failure to maintain an adequate record on an individual, when the result is a determination "adverse" to that person. Subsection (g)(1)(D) speaks of a violation when someone suffers an "adverse effect" from any other failure to hew to the terms of the Act. Like the inspection and correction infractions, breaches of the statute with adverse consequences are addressed by specific terms governing relief:

> "In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—
>
> "(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and
>
> "(B) the costs of the action together with reasonable attorney fees as determined by the court." § 552a(g)(4).

Doe argues that subsection (g)(4)(A) entitles any plaintiff adversely affected by an intentional or willful violation to the $1,000 minimum on proof of nothing more than a statutory violation: anyone suffering an adverse consequence of intentional or willful disclosure is entitled to recovery. The Government claims the minimum guarantee goes only to victims who prove some actual damages. We think the Government has the better side of the argument.

To begin with, the Government's position is supported by a straightforward textual analysis. When the statute gets to the point of guaranteeing the $1,000 minimum, it not only has confined any eligibility to victims of adverse effects caused by intentional or willful actions, but has provided expressly for liability to such victims for "actual damages sustained." It has made specific provision, in other words, for what a victim within the limited class may recover. When the very next clause of the sentence containing the explicit provision guarantees $1,000 to a "person entitled to recovery," the simplest reading of that phrase looks back to the immediately preceding provision for recovering actual damages, which is also the Act's sole provision for recovering anything (as distinct from equitable relief). With such an obvious referent for "person entitled to recovery" in the plaintiff who sustains "actual damages," Doe's theory is immediately questionable in ignoring the "actual damages" language so directly at hand and instead looking for "a person entitled to recovery" in a separate part of the statute devoid of any mention either of recovery or of what might be recovered.

Nor is it too strong to say that Doe does ignore statutory language. When Doe reads the statute to mean that the United States shall be liable to any adversely affected subject of an intentional or willful violation, without more, he treats willful action as the last fact necessary to make the Government "liable," and he is thus able to describe anyone to whom it is liable as entitled to the $1,000 guarantee. But this way of reading the statute simply pays no attention to the fact that the statute does not speak of liability (and consequent entitlement to recovery) in a freestanding, unqualified way, but in a limited way, by reference to enumerated damages.

Doe's manner of reading "entitle[ment] to recovery" as satisfied by adverse effect caused by intentional or willful violation is in tension with more than the text, however. It is at odds with the traditional understanding that tort recovery requires not only wrongful act plus causation reaching to the plaintiff, but proof of some harm for which damages can reasonably be assessed. Doe, instead, identifies a person as entitled to recover without any reference to proof of damages, actual or otherwise. Doe might respond that it makes sense to speak of a privacy tort victim as entitled to recover without reference to damages because analogous common law would not require him to show particular items of injury in order to receive a dollar recovery. Traditionally, the common law has provided such victims with a claim for "general" damages, which for privacy and defamation torts are presumed damages: a monetary award calculated without reference to specific harm.

Congress cut out the very language in the bill that would have authorized any presumed damages. The Senate bill would have authorized an award of "actual and general damages sustained by any person," with that language followed by the guarantee that "in no case shall a person entitled to recovery receive less than the sum of $1,000." Although the provision for general damages would have covered presumed damages, this language was trimmed from the final statute, subject to any later revision that might be recommended by the Commission. The deletion of "general damages" from the bill is fairly seen, then, as a deliberate elimination of any possibility of imputing harm and awarding presumed damages. The deletion thus precludes any hope of a sound interpretation of entitlement to recovery without reference to actual damages.

Finally, Doe's reading is open to the objection that no purpose is served by conditioning the guarantee on a person's being entitled to recovery. As Doe treats the text, Congress could have accomplished its object simply by providing that the Government would be liable to the individual for actual damages "but in no case . . . less than the sum of $1,000" plus fees and costs. Doe's reading leaves the reference to entitlement to recovery with no job to do, and it accordingly accomplishes nothing.

There are three loose ends. Doe's argument suggests it would have been illogical for Congress to create a cause of action for anyone who suffers an adverse effect from intentional or willful agency action, then deny recovery without actual damages. But this objection assumes that the language in subsection (g)(1)(D) recognizing a federal "civil action" on the part of someone adversely affected was meant, without more, to provide a complete cause of action, and of course this is not so. A subsequent provision requires proof of intent or willfulness in addition to adverse effect, and if the specific state of mind must be proven additionally, it is equally consistent with logic to require some actual damages as well.

Next, Doe also suggests there is something peculiar in offering some guaranteed damages, as a form of presumed damages not requiring proof of amount, only to those plaintiffs who can demonstrate actual damages. But this approach parallels another remedial scheme that the drafters of the Privacy Act would probably have known about. At common law, certain defamation torts were redressed by general damages but only when a plaintiff first proved some "special harm," *i.e.,* "harm of a material and generally of a pecuniary nature." Plaintiffs claiming such torts could recover presumed damages only if they could demonstrate some actual, quantifiable pecuniary loss. Because the recovery of presumed damages in these cases was supplemental to compensation for specific harm, it was hardly unprecedented for Congress to

make a guaranteed minimum contingent upon some showing of actual damages, thereby avoiding giveaways to plaintiffs with nothing more than "abstract injuries."

The "entitle[ment] to recovery" necessary to qualify for the $1,000 minimum is not shown merely by an intentional or willful violation of the Act producing some adverse effect. The statute guarantees $1,000 only to plaintiffs who have suffered some actual damages. [12] The judgment of the Fourth Circuit is affirmed.

Justice GINSBURG, with whom Justice STEVENS and Justice BREYER join, dissenting.

In this Privacy Act suit brought under 5 U.S.C. § 552a(g)(1)(D), the Government concedes the alleged violation and does not challenge the District Court's finding that the agency in question (the Department of Labor) acted in an intentional or willful manner. Nor does the Government here contest that Buck Doe, the only petitioner before us, suffered an "adverse effect" from the Privacy Act violation. The case therefore cleanly presents a sole issue for this Court's resolution: Does a claimant who has suffered an "adverse effect"—in this case and typically, emotional anguish—from a federal agency's intentional or willful Privacy Act violation, but has proved no "actual damages" beyond psychological harm, qualify as "a person entitled to recovery" within the meaning of § 552a(g)(4)(A)? I would answer that question yes.

The words "a person entitled to recovery," as used in § 552a(g)(4)(A)'s remedial prescription, are most sensibly read to include anyone experiencing an "adverse effect" as a consequence of an agency's intentional or willful commission of a Privacy Act violation of the kind described in § 552a(g)(1)(C) or (D).

"It is 'a cardinal principle of statutory construction' that 'a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant.'" The Court's reading of § 552a(g)(4) is hardly in full harmony with that principle. Under the Court's construction, the words "a person entitled to recovery" have no office and the liability-determining element "adverse effect" becomes superfluous, swallowed up by the "actual damages" requirement. Further, the Court's interpretation renders the word "recovery" nothing more than a synonym for "actual damages," and it turns the phrase "shall be liable" into "may be liable." In part because it fails to "give effect . . . to every clause and word" Congress wrote, the Court's reading of § 552a(g)(4) is at odds with the interpretation prevailing in the Federal Circuits.

The purpose and legislative history of the Privacy Act, as well as similarly designed statutes, are in harmony with the reading of § 552a(g)(4) most federal judges have found sound. Congress sought to afford recovery for "*any* damages" resulting from the "willful or intentional" violation of "any individual's rights under th[e] Act." § 2(b)(6), 88 Stat. 1896 (emphasis added). Privacy Act violations commonly cause fear, anxiety, or other emotional distress—in the Act's parlance, "adverse effects." Harm of this character must, of course, be proved genuine. In cases like Doe's, emotional distress is generally the only harm the claimant suffers, *e.g.,* the identity theft apprehended never materializes.

The Court's reading of § 552a(g)(4) to require proof of "actual damages," however small, in order to gain the $1,000 statutory minimum, ironically, invites claimants to arrange or manufacture such damages. The following colloquy from oral argument is illustrative.

> Court: "Suppose . . . Doe said, 'I'm very concerned about the impact of this on my credit rating, so I'm going to [pay] $10 to a . . . credit reporting company to find

[12] The Courts of Appeals are divided on the precise definition of actual damages. That issue is not before us, however . . . . We assume without deciding that the Fourth Circuit was correct to hold that Doe's complaints in this case did not rise to the level of alleging actual damages. We do not suggest that out-of-pocket expenses are necessary for recovery of the $1,000 minimum; only that they suffice to qualify under any view of actual damages.

> out whether there's been any theft of my identity, $10.' Would there then be a claim under this statute for actual damages?"
>
> Counsel for respondent Secretary of Labor Chao: "[T]here would be a question . . . whether that was a reasonable response to the threat, but in theory, an expense like that could qualify as pecuniary harm and, thus, is actual damages."

Indeed, the Court itself suggests that "fees associated with running a credit report" or "the charge for a Valium prescription" might suffice to prove "actual damages." I think it dubious to insist on such readily created costs as essential to recovery under § 552a(g)(4). Nevertheless, the Court's examples of what might qualify as "actual damages" indicate that its disagreement with the construction of the Act prevailing in the Circuits is ethereal.

The Government, although recognizing that "actual damages" may be slender and easy to generate, fears depletion of the federal fisc were the Court to adopt Doe's reading of § 552a(g)(4). Experience does not support those fears. As the Government candidly acknowledged at oral argument: "[W]e have not had a problem with enormous recoveries against the Government up to this point." No doubt mindful that Congress did not endorse massive recoveries, the District Court in this very case denied class-action certification and other courts have similarly refused to certify suits seeking damages under § 552a(g)(4) as class actions. Furthermore, courts have disallowed the runaway liability that might ensue were they to count every single wrongful disclosure as a discrete basis for a $1,000 award.

The text of § 552a(g)(4), it is undisputed, accommodates two concerns. Congress sought to give the Privacy Act teeth by deterring violations and providing remedies when violations occur. At the same time, Congress did not want to saddle the Government with disproportionate liability. The Senate bill advanced the former concern; the House bill was more cost conscious.

The provision for monetary relief ultimately enacted, § 552a(g)(4), represented a compromise between the House and Senate versions. The House bill's culpability standard ("willful, arbitrary, or capricious"), not present in the Senate bill, accounts for § 552a(g)(4)'s imposition of liability only when the agency acts in an "intentional or willful" manner. That culpability requirement affords the Government some insulation against excessive liability. On the other hand, the enacted provision adds to the House allowance of "actual damages" only, the Senate specification that "in no case shall a person entitled to recovery receive less than the sum of $1,000 . . . ." § 552a(g)(4)(A). The $1,000 minimum enables individuals to recover for genuine, albeit nonpocketbook, harm, and gives persons thus adversely affected an incentive to sue to enforce the Act.

Congress has used language similar to § 552a(g)(4) in other privacy statutes. These other statutes have been understood to permit recovery of the $1,000 statutory minimum despite the absence of proven actual damages. See H.R.Rep. No. 99–647 (1986) ("Damages [under 18 U.S.C. § 2707(c)] include actual damages, any lost profits but in no case less than $1,000."); S.Rep. No. 99–541 (1986), ("[D]amages under [18 U.S.C. § 2707(c)] includ[e] the sum of actual damages suffered by the plaintiff and any profits made by the violator as the result of the violation . . . with minimum statutory damages of $1,000 . . . and . . . reasonable attorney's fees and other reasonable litigation costs."); H.R. Conf. Rep. No. 94–1515 (1976), (Title 26 U.S.C. § 6110(j)(2) "creates a civil remedy for intentional or willful failure of the IRS to make required deletions or to follow the procedures of this section, including minimum damages of $1,000 plus costs."). As Circuit Judge Michael, dissenting from the Fourth Circuit's disposition of Doe's claim, trenchantly observed: "[T]he remedy of minimum statutory damages is a fairly common feature of federal legislation . . . . In contrast, I am not aware of any statute in which Congress has provide[d] for a statutory minimum to actual damages."

Doe has standing to sue, the Court agrees, based on "allegations that he was 'torn . . . all to pieces' and 'greatly concerned and worried' because of the disclosure of his Social Security number and its potentially 'devastating' consequences." Standing to sue, but not to succeed, the

Court holds, unless Doe also incurred an easily arranged out-of-pocket expense. In my view, Congress gave Privacy Act suitors like Doe not only standing to sue, but the right to a recovery if the fact trier credits their claims of emotional distress brought on by an agency's intentional or willful violation of the Act. For the reasons stated in this dissenting opinion, which track the reasons expressed by Circuit Judge Michael dissenting in part in the Fourth Circuit, I would reverse the judgment of the Court of Appeals.

Notes

1. In both this case and the following one the majority appears concerned about making the government liable for damages too frequently for inconsequential violations of privacy. Consider the nature of government records. The government has data on every American. It could easily violate the privacy of 300 million people through a single act of misconduct. Such errors could be the basis of massive class actions. As the dissenters point out, mere government negligence is not enough to create liability; a higher mens rea is required. Nevertheless, the majority is concerned.
2. Ginsburg speculates that it would not be difficult for a clever plaintiff (or, more likely, a clever plaintiff's lawyer) to turn a bare allegation of emotional harm into a clear financial injury, such as a therapy bill. This possibility is addressed in *F.A.A. v. Cooper*.

F.A.A. v. Cooper, 566 U.S. 284 (2012)

Justice ALITO delivered the opinion of the Court.

The Federal Aviation Administration (FAA) requires pilots to obtain a pilot certificate and medical certificate as a precondition for operating an aircraft. Pilots must periodically renew their medical certificates to ensure compliance with FAA medical standards. When applying for renewal, pilots must disclose any illnesses, disabilities, or surgeries they have had, and they must identify any medications they are taking.

Respondent Stanmore Cooper has been a private pilot since 1964. In 1985, he was diagnosed with a human immunodeficiency virus (HIV) infection and began taking antiretroviral medication. At that time, the FAA did not issue medical certificates to persons with respondent's condition. Knowing that he would not qualify for renewal of his medical certificate, respondent initially grounded himself and chose not to apply. In 1994, however, he applied for and received a medical certificate, but he did so without disclosing his HIV status or his medication. He renewed his certificate in 1998, 2000, 2002, and 2004, each time intentionally withholding information about his condition.

When respondent's health deteriorated in 1995, he applied for long-term disability benefits under Title II of the Social Security Act. To substantiate his claim, he disclosed his HIV status to the Social Security Administration (SSA), which awarded him benefits for the year from August 1995 to August 1996.

In 2002, the Department of Transportation (DOT), the FAA's parent agency, launched a joint criminal investigation with the SSA, known as "Operation Safe Pilot," to identify medically unfit individuals who had obtained FAA certifications to fly. The DOT gave the SSA a list of names and other identifying information of 45,000 licensed pilots in northern California. The SSA then compared the list with its own records of benefit recipients and compiled a spreadsheet, which it gave to the DOT.

The spreadsheet revealed that respondent had a current medical certificate but had also received disability benefits. After reviewing respondent's FAA medical file and his SSA disability file, FAA flight surgeons determined in 2005 that the FAA would not have issued a medical certificate to respondent had it known his true medical condition.

When investigators confronted respondent with what had been discovered, he admitted that he had intentionally withheld from the FAA information about his HIV status and other relevant medical information. Because of these fraudulent omissions, the FAA revoked respondent's pilot certificate, and he was indicted on three counts of making false statements to a Government agency.

Claiming that the FAA, DOT, and SSA (hereinafter Government) violated the Privacy Act by sharing his records with one another, respondent filed suit in the United States District Court for the Northern District of California. He alleged that the unlawful disclosure to the DOT of his confidential medical information, including his HIV status, had caused him "humiliation, embarrassment, mental anguish, fear of social ostracism, and other severe emotional distress."

The civil remedies provision of the Privacy Act provides that, for any "intentional or willful" refusal or failure to comply with the Act, the United States shall be liable for "actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000." Because Congress did not define "actual damages," respondent urges us to rely on the ordinary meaning of the word "actual" as it is defined in standard general-purpose dictionaries. But as the Court of Appeals explained, "actual damages" is a legal term of art, and it is a "cardinal rule of statutory construction" that, when Congress employs a term of art, "it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken."

Because the term "actual damages" has this chameleon-like quality, we cannot rely on any all-purpose definition but must consider the particular context in which the term appears.

The Privacy Act directs agencies to establish safeguards to protect individuals against the disclosure of confidential records "which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." Because the Act serves interests similar to those protected by defamation and privacy torts, there is good reason to infer that Congress relied upon those torts in drafting the Act.

In *Doe v. Chao* (2004), we held that the Privacy Act's remedial provision authorizes plaintiffs to recover a guaranteed minimum award of $1,000 for violations of the Act, but only if they prove at least some "actual damages." Although we did not address the meaning of "actual damages," we observed that the provision "parallels" the remedial scheme for the common-law torts of libel *per quod* and slander, under which plaintiffs can recover "general damages," but only if they prove "special harm" (also known as "special damages"). "Special damages" are limited to actual pecuniary loss, which must be specially pleaded and proved. "General damages," on the other hand, cover "loss of reputation, shame, mortification, injury to the feelings and the like and need not be alleged in detail and require no proof."

This parallel between the Privacy Act and the common-law torts of libel *per quod* and slander suggests the possibility that Congress intended the term "actual damages" in the Act to mean special damages. The basic idea is that Privacy Act victims, like victims of libel *per quod* or slander, are barred from any recovery unless they can first show actual—that is, pecuniary or material—harm. Upon showing some pecuniary harm, no matter how slight, they can recover the statutory minimum of $1,000, presumably for any unproven harm. That Congress would choose to use the term "actual damages" instead of "special damages" was not without precedent. The terms had occasionally been used interchangeably.

Any doubt about the plausibility of construing "actual damages" in the Privacy Act synonymously with "special damages" is put to rest by Congress' refusal to authorize "general damages." In an uncodified section of the Act, Congress established the Privacy Protection Study Commission to consider, among other things, "whether the Federal Government should be liable for general damages." As we explained in *Doe,* "Congress left the question of general

damages . . . for another day." Although the Commission later recommended that general damages be allowed, Congress never amended the Act to include them.

By authorizing recovery for "actual" but not for "general" damages, Congress made clear that it viewed those terms as mutually exclusive.

We do not claim that the contrary reading of the statute accepted by the Court of Appeals and advanced now by respondent is inconceivable. But because the Privacy Act waives the Federal Government's sovereign immunity, the question we must answer is whether it is plausible to read the statute, as the Government does, to authorize only damages for economic loss. When waiving the Government's sovereign immunity, Congress must speak unequivocally. Here, we conclude that it did not. As a consequence, we adopt an interpretation of "actual damages" limited to proven pecuniary or economic harm. To do otherwise would expand the scope of Congress' sovereign immunity waiver beyond what the statutory text clearly requires.

None of respondent's contrary arguments suffices to overcome the sovereign immunity canon.

Respondent notes that the term "actual damages" has often been defined broadly in common-law cases, and in our own, to include all compensatory damages. For example, in *Birdsall v. Coolidge* (1876), a patent infringement case, we observed that "[c]ompensatory damages and actual damages mean the same thing." And in *Gertz v. Robert Welch, Inc.* (1974), we wrote that actual injury in the defamation context "is not limited to out-of-pocket loss" and that it customarily includes "impairment of reputation and standing in the community, personal humiliation, and mental anguish and suffering."

These cases and others cited by respondent stand for the unremarkable point that the term "actual damages" *can* include nonpecuniary loss. But this generic meaning does not establish with the requisite clarity that the Privacy Act, with its distinctive features, authorizes damages for mental and emotional distress. As we already explained, the term "actual damages" takes on different meanings in different contexts.

Respondent's stronger argument is that the exclusion of "general damages" from the statute simply means that there can be no recovery for presumed damages. Privacy Act victims can still recover for mental and emotional distress, says respondent, so long as it is proved.

This argument is flawed because it suggests that *proven* mental and emotional distress does not count as general damages. The term "general damages" is not limited to compensation for unproven injuries; it includes compensation for proven injuries as well. To be sure, specific proof of emotional harm is not required to recover general damages for dignitary torts. But it does not follow that general damages cannot be recovered for emotional harm that is actually proved.

Aside from the fact that general damages need not be proved, what distinguishes those damages, whether proved or not, from the only other category of compensatory damages available in the relevant common-law suits is the *type* of harm. In defamation and privacy cases, "the affront to the plaintiff's dignity and the emotional harm done" are "called general damages, to distinguish them from proof of actual economic harm," which is called "special damages." Therefore, the converse of general damages is special damages, not all proven damages, as respondent would have it. Because Congress removed "general damages" from the Act's remedial provision, it is reasonable to infer that Congress foreclosed recovery for nonpecuniary harm, even if such harm can be proved, and instead waived the Government's sovereign immunity only with respect to harm compensable as special damages.

Finally, respondent argues that excluding damages for mental and emotional harm would lead to absurd results. Persons suffering relatively minor pecuniary loss would be entitled to recover $1,000, while others suffering only severe and debilitating mental or emotional distress would get nothing.

Contrary to respondent's suggestion, however, there is nothing absurd about a scheme that limits the Government's Privacy Act liability to harm that can be substantiated by proof of tangible economic loss. Respondent insists that such a scheme would frustrate the Privacy Act's remedial purpose, but that ignores the fact that, by deliberately refusing to authorize general damages, Congress intended to cabin relief, not to maximize it.

In sum, applying traditional rules of construction, we hold that the Privacy Act does not unequivocally authorize an award of damages for mental or emotional distress. Accordingly, the Act does not waive the Federal Government's sovereign immunity from liability for such harms.

Justice SOTOMAYOR, with whom Justice GINSBURG and Justice BREYER join, dissenting.

Today the Court holds that "actual damages" is limited to pecuniary loss. Consequently, individuals can no longer recover what our precedents and common sense understand to be the primary, and often only, damages sustained as a result of an invasion of privacy, namely, mental or emotional distress. That result is at odds with the text, structure, and drafting history of the Act. And it cripples the Act's core purpose of redressing and deterring violations of privacy interests. I respectfully dissent.

The majority concludes that "actual damages" in the civil-remedies provision of the Privacy Act allows recovery for pecuniary loss alone. But it concedes that its interpretation is not compelled by the plain text of the statute or otherwise required by any other traditional tool of statutory interpretation. And it candidly acknowledges that a contrary reading is not "inconceivable." Yet because it considers its reading of "actual damages" to be "plausible," the majority contends that the canon of sovereign immunity requires adoption of an interpretation most favorable to the Government.

The canon simply cannot bear the weight the majority ascribes it. "The sovereign immunity canon is just that—a canon of construction. It is a tool for interpreting the law, and we have never held that it displaces the other traditional tools of statutory construction." *Richlin Security Service Co. v. Chertoff* (2008) (opinion of ALITO, J.). Here, traditional tools of statutory construction—the statute's text, structure, drafting history, and purpose—provide a clear answer: The term "actual damages" permits recovery for all injuries established by competent evidence in the record, whether pecuniary or nonpecuniary, and so encompasses damages for mental and emotional distress. There is no need to seek refuge in a canon of construction, much less one that has been used so haphazardly in the Court's history.

I turn finally to the statute's purpose, for "[a]s in all cases of statutory construction, our task is to interpret the words of th[e] statut[e] in light of the purposes Congress sought to serve." The purposes of the Privacy Act could not be more explicit, and they are consistent with interpreting "actual damages" according to its ordinary meaning.

Reading "actual damages" to permit recovery for any injury established by competent evidence in the record—pecuniary or not—best effectuates the statute's basic purpose. Although some privacy invasions no doubt result in economic loss, we have recognized time and again that the primary form of injuries is nonpecuniary, and includes mental distress and personal humiliation.

In interpreting the civil-remedies provision, we must not forget Congress enacted the Privacy Act to protect privacy. The majority's reading of "actual damages" renders the remedial provision impotent in the face of concededly unlawful agency action whenever the injury is solely nonpecuniary. That result is patently at odds with Congress' stated purpose. The majority, however, does not grapple with the ramifications of its opinion. It acknowledges the suggestion that its holding leads to absurd results as it allows individuals suffering relatively minor pecuniary losses to recover $1,000 while others suffering severe mental anguish to

recover nothing. But it concludes that "there is nothing absurd about a scheme that limits the Government's Privacy Act liability to harm that can be substantiated by proof of tangible economic loss."

After today, no matter how debilitating and substantial the resulting mental anguish, an individual harmed by a federal agency's intentional or willful violation of the Privacy Act will be left without a remedy unless he or she is able to prove pecuniary harm. That is not the result Congress intended when it enacted an Act with the express purpose of safeguarding individual privacy against Government invasion. And it is not a result remotely suggested by anything in the text, structure, or history of the Act. For those reasons, I respectfully dissent.

Notes

1. The district court in *Cooper* also evaluated whether the sharing of information was a routine use. It held that it was not. This may seem like a surprising result given the potential breadth of the "routine use" exception, but – as mentioned above – courts evaluate routine uses with respect to the disclosures made in the Federal Register. In *Cooper v. F.A.A* (N.D. Cal. 2008), the court said:

   > Routine use 1 allows sharing with an appropriate federal agency only when a system of DOT records "indicates a violation or potential violation of the law." When DOT–OIG sent the name, social security number, date of birth and gender of approximately 45,000 pilots to SSA–OIG, it was not because those records indicated a violation or potential violation of the law. Rather, the records were sent to discover violations or potential violations.
   >
   > And while routine use 9 allows sharing of records for law enforcement activities "regardless of the stated purpose for the collection of the information," it only allows the disclosure of names. DOT–OIG's sharing of social security numbers, dates of birth and gender is clearly beyond the scope of this routine use.

2. The majority in *Cooper* is clear that even proven emotional damages do not count as actual damages under the Privacy Act, forestalling the clever tricks that appeared possible in *Doe*.
3. In addition to the problem of proving actual damages, plaintiffs under the Privacy Act also struggle to prove the requisite mens rea. Recall that the standard is "intentional or willful." Though an exact definition has proven elusive, the 10th Circuit set out some helpful markers in *Andrews v. Veterans Admin. of U.S.* (1988), a case that involved the release of insufficiently anonymized performance reviews:

   > [P]remeditated malice is not required to establish a willful or intentional violation of the Privacy Act. Nonetheless, the term "willful or intentional" clearly requires conduct amounting to more than gross negligence. We are persuaded by the District of Columbia Circuit's definitions of willful or intentional that contemplate action "so 'patently egregious and unlawful' that anyone undertaking the conduct should have known it 'unlawful'" or conduct committed "without grounds for believing it to be lawful" or action "flagrantly disregarding others' rights under the Act," and we adopt those definitions, and add the view expressed in *Moskiewicz* (7th Cir. 1986), that the conduct must amount to, at the very least, reckless behavior. Those, and similar definitions, describe conduct more extreme than gross negligence.

   There, the court held that the actions did not amount to gross negligence as the staffer at issue made a good faith—if apparently not fully competent— attempt to redact identifiable information.

In re U.S. OPM Data Security Breach Litig., 928 F.3d 42 (D.C. Cir. 2019)

Per Curiam:

In 2014, cyberattackers breached multiple U.S. Office of Personnel Management ("OPM") databases and allegedly stole the sensitive personal information—including birth dates, Social Security numbers, addresses, and even fingerprint records—of a staggering number of past, present, and prospective government workers. All told, the data breaches affected more than twenty-one million people. Unsurprisingly, given the scale of the attacks and the sensitive nature of the information stolen, news of the breaches generated not only widespread alarm, but also several lawsuits. These suits were ultimately consolidated into two complaints: one filed by the National Treasury Employees Union and three of its members, and another filed by the American Federation of Government Employees on behalf of several individual plaintiffs and a putative class of others similarly affected by the breaches. Both sets of plaintiffs alleged that OPM's cybersecurity practices were woefully inadequate, enabling the hackers to gain access to the agency's treasure trove of employee information, which in turn exposed plaintiffs to a heightened risk of identity theft and a host of other injuries.

As its name suggests, the U.S. Office of Personnel Management serves as the federal government's chief human resources agency. In that capacity, OPM maintains electronic personnel files that contain, among other information, copies of federal employees' birth certificates, military service records, and job applications identifying Social Security numbers and birth dates.

The agency also oversees more than two million background checks and security clearance investigations per year. To facilitate these investigations, OPM collects a tremendous amount of sensitive personal information from current and prospective federal workers, most of which it then stores electronically in a "Central Verification System." In recent years, OPM has relied on a private investigation and security firm, KeyPoint Government Solutions, Inc. ("KeyPoint"), to conduct the lion's share of the agency's background and security clearance investigation fieldwork. KeyPoint investigators have access to the information stored in OPM's Central Verification System and can transmit data to and from the agency's network through an electronic portal.

It turns out that authorized KeyPoint investigators have not been the only third parties to access OPM's data systems. Cyberattackers hacked into the agency's network on several occasions between November 2013 and November 2014. Undetected for months, at least two of these breaches resulted in the theft of vast quantities of personal information. According to the complaint, after breaching OPM's network "using stolen KeyPoint credentials" around May 2014, the cyberintruders extracted almost 21.5 million background investigation records from the agency's Central Verification System. They gained access to another OPM system near the end of 2014, stealing over four million federal employees' personnel files. Among the types of information compromised were current and prospective employees' Social Security numbers, birth dates, and residency details, along with approximately 5.6 million sets of fingerprints. The breaches also exposed the Social Security numbers and birth dates of the spouses and cohabitants of those who, in order to obtain a security clearance, completed a Standard Form 86. According to the complaints, since these 2014 breaches, individuals whose information was stolen have experienced incidents of financial fraud and identity theft; many others whose information has not been misused—at least, not yet—remain concerned about the ongoing risk that they, too, will become victims of financial fraud and identity theft in the future.

After announcing the breaches in the summer of 2015, OPM initially offered individuals whose information had been compromised fraud monitoring and identity theft protection services and insurance at no cost for either eighteen months or three years, depending on whether their Social Security numbers had been exposed. But OPM's offer failed to address the

concerns of all such parties, and the agency soon found itself named as a defendant in breach-related lawsuits across the country.

"Arnold Plaintiffs" allege that KeyPoint's "information security defenses did not conform to recognized industry standards" and that the company unreasonably failed to protect the security credentials that the hackers used to unlawfully access one of OPM's systems in mid-2014. Specifically, they assert that "KeyPoint knew or should have known that its information security defenses did not reasonably or effectively protect Plaintiffs' and Class members' [personal information] and the credentials used to access it on KeyPoint's and OPM's systems." As for OPM, Arnold Plaintiffs allege that the agency had long been on notice that its systems were prime targets for cyberattackers. OPM experienced data breaches related to cyberattacks in 2009 and 2012, and it is no secret that its network is regularly subject to a strikingly large number of hacking attempts. Despite this, say Arnold Plaintiffs, OPM repeatedly failed to comply with the Federal Information Security Management Act of 2002 (repealed 2014), and its replacement, the Federal Information Security Modernization Act of 2014 (collectively, "Information Security Act"), which require agencies to "develop, implement, and maintain a security program that assesses information security risks and provides adequate security for the operations and assets of programs and software systems under agency and contractor control."

As early as 2007, Information Security Act compliance audits conducted by OPM's Office of the Inspector General regularly identified major information security deficiencies that left the agency's network vulnerable to attack. Such problems included "severely outdated" security policies and procedures, understaffed and undertrained cybersecurity personnel, and a lack of a centralized information security management structure. As a result, in every year from 2007 through 2013, the Inspector General identified "serious concerns that * * * pose an immediate risk to the security of assets or operations"—termed "material weaknesses"—in the agency's information security governance program. Although in 2014 the Inspector General, acting on the basis of "imminently planned improvements," reclassified OPM's security governance program as a "significant deficiency" (an improvement over the more serious "material weakness"), other serious issues resurfaced at that time.

The 2014 cyberattacks were "sophisticated, malicious, and carried out to obtain sensitive information for improper use." Arnold Plaintiffs assert that as a result of these attacks, they have suffered from a variety of harms, including the improper use of their Social Security numbers, unauthorized charges to existing credit card and bank accounts, fraudulent openings of new credit card and other financial accounts, and the filing of fraudulent tax returns in their names. At least three named Arnold Plaintiffs purchased credit monitoring services after falling victim to such fraud; others have spent time and money attempting to unwind fraudulent transactions made in their names. And some Arnold Plaintiffs who have yet to experience a fraud incident purchased credit monitoring services and spent extra time monitoring their accounts to mitigate the "increased risk" of identity theft caused by the breaches.

The Privacy Act waives sovereign immunity by expressly authorizing a cause of action for damages against federal agencies that violate its rules protecting the confidentiality of private information in agency records.

The district court nonetheless ruled that OPM's sovereign immunity remained intact, reasoning that Arnold Plaintiffs failed to allege the type of harms covered by the Privacy Act. Reviewing the district court's dismissal of the Privacy Act claim *de novo*, we reverse. OPM's allegedly willful failure to protect Arnold Plaintiffs' sensitive personal information against the theft that occurred falls squarely within the Privacy Act's ambit.

To start, Arnold Plaintiffs have straightforwardly alleged a "willful" violation of the Privacy Act's requirements. OPM was necessarily aware that the Privacy Act requires it to "establish appropriate administrative, technical, and physical safeguards" that "insure the

security and confidentiality of records," and to "protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

The complaint alleges in no uncertain terms that OPM dropped that ball because appropriate safeguards were not in place. *See, e.g.*, Arnold Plaintiffs' Compl. ("OPM's decisions not to comply with [Information Security Act] requirements for critical security safeguards enabled hackers to access and loot OPM's systems for nearly a year without being detected."); ("Despite known and persistent threats from cyberattacks, OPM allowed multiple 'material weaknesses' in its information security systems to continue unabated. As a result, Plaintiffs' and Class members' [government investigation information] under OPM's control was exposed, stolen, and misused.").

Of course, violating the Privacy Act is not by itself enough. The agency's transgression must have been "intentional or willful." Under the Privacy Act, willfulness means more than "gross negligence." Allegations that the agency's conduct was "disjointed" or "confused," or that errors were "inadvertent[ ]" will not suffice.

Instead, a complaint must plausibly allege that the agency's security failures were "in flagrant disregard of [their] rights under the Act," were left in place "without grounds for believing them to be lawful," or were "so patently egregious and unlawful that anyone undertaking the conduct should have known it unlawful."

Arnold Plaintiffs' complaint clears that hurdle by plausibly and with specificity alleging that OPM was willfully indifferent to the risk that acutely sensitive private information was at substantial risk of being hacked. According to the complaint, at the time of the breach, OPM had long known that its electronic record-keeping systems were prime targets for hackers. The agency suffered serious data breaches from hackers in 2009 (millions of users' personal information stolen) and 2012 (OPM access credentials stolen and posted online), and is subject to at least *ten million* unauthorized electronic intrusion attempts *every month*.

Despite that pervading threat, OPM effectively left the door to its records unlocked by repeatedly failing to take basic, known, and available steps to secure the trove of sensitive information in its hands. Information Security Act audits by OPM's Inspector General repeatedly warned OPM about material deficiencies in its information security systems. Among the identified flaws were

- severely outdated security policies and procedures;
- permitting employees to leave open, or to not terminate, remote access;
- understaffed and undertrained cybersecurity personnel;
- failure to implement or enforce multi-factor identification in *any* of its major information systems;
- declining to patch or install security updates for its systems promptly;
- lacking a mature vulnerability scanning program to find and track the status of security weaknesses in its systems;
- failure to maintain a centralized information security management structure that would continuously monitor security events and controls;
- lacking the ability to detect unauthorized devices connected to its network; and
- failure to engage in appropriate oversight of its contractor-operated systems.

So forewarned, OPM chose to leave those critical information security deficiencies (and more) in place. On top of that, in the year that the hacks occurred, OPM (allegedly) also left undone mandated security assessments and authorizations for half of its electronic record-keeping systems. The risk created by these lapses was so serious that the Inspector General took the unprecedented step of advising OPM to shut down all the systems lacking valid authorizations until adequate security measures could be put in place. OPM declined, choosing instead to continue operating these systems.

The complaint's plausible allegations that OPM decided to continue operating in the face of those repeated and forceful warnings, without implementing even the basic steps needed to minimize the risk of a significant data breach, is precisely the type of willful failure to establish appropriate safeguards that makes out a claim under the Privacy Act.

Arnold Plaintiffs' lawsuit is not in the clear yet. The complaint must also allege facts showing that they suffered "actual damages" as "a result of" OPM's Privacy Act violation. The complaint rises to that task as well.

"Actual damages" within the meaning of the Privacy Act are limited to proven pecuniary or economic harm. *Federal Aviation Admin. v. Cooper* (2012). The district court concluded that only two Arnold Plaintiffs had properly alleged that they suffered "actual damages": Jane Doe, who incurred legal fees when she retained a law firm to close fraudulent accounts opened in her name, and Charlene Oliver, whose electricity account had been fraudulently accessed and saddled with unauthorized charges.

While those harms certainly qualify as actual damages, the complaint contains still more relevant allegations of injury.

First, nine of the named Arnold Plaintiffs purchased credit protection and/or credit repair services after learning of the breach. Paul Daly, for example, purchased credit monitoring services after a fraudulent 2014 tax return was filed in his name. And Teresa J. McGarry subscribed to a monthly credit and identity protection service to prevent identity theft. Those reasonably incurred out-of-pocket expenses are the paradigmatic example of "actual damages" resulting from the violation of privacy protections. *Cooper*.

OPM counters that those individual purchases were unnecessary because Congress provided credit monitoring services for potentially affected individuals. Congress, though, did not offer credit repair services. Anyhow, the argument wrongly assumes facts in OPM's favor at the complaint stage, such as that the services offered were equal or superior to those obtained privately, or that they took effect in a timely manner and for a sufficient period of time. Notably, at least one named plaintiff purchased credit monitoring services *before* OPM's offered services were "up and running."

Second, seven of the named Arnold Plaintiffs had accounts opened and purchases made in their names. For example, Kelly Flynn and her husband had several new credit card accounts fraudulently opened in their names. They also discovered that two separate loans totaling $6,400 had been taken out in their names without their permission and were now delinquent. Those financial losses qualify as "actual damages."

The district court deemed those damages insufficient because Arnold Plaintiffs did not further allege that their costs went unreimbursed. That was error. At this stage of the litigation, all facts and reasonable inferences must be drawn in favor of Arnold Plaintiffs, and the complaint provides no basis for disregarding the claimed financial losses based on OPM's speculation that Arnold Plaintiffs were indemnified.

Anyhow, "an injured person may usually recover in full from a wrongdoer regardless of anything he may get from a collateral source unconnected with the wrongdoer." That rule prevents the victim's benefits from becoming the tortfeasor's windfall. So too here.

Third, Plaintiffs Kelly Flynn and six others had false tax returns filed using their information and have experienced delays in receiving federal and state tax refunds. The delay in those Plaintiffs' receipt of their refunds, and the forgone time value of that money, is an actual, tangible pecuniary injury.

Lastly, one Plaintiff, Lillian Gonzalez-Colon, spent more than 100 hours to resolve the fraudulent tax return filing and to close a fraudulently opened account. Those efforts "required her to take time off work[ ]" to address the consequences of the OPM breach.

For all of those reasons, Arnold Plaintiffs have adequately alleged actual damages within the meaning of the Privacy Act.

The complaint also explains how Arnold Plaintiffs' actual damages were the "result of" OPM's Privacy Act violations. 5 U.S.C. § 552a(g)(4)(A).

To meet the Privacy Act's causation requirement, Arnold Plaintiffs must plausibly allege that the OPM hack was the "proximate cause" of their damages. That is, OPM's conduct must have been a "substantial factor" in the sequence of events leading to Arnold Plaintiffs' injuries, and those injuries must have been "reasonably foreseeable or anticipated as a natural consequence" of OPM's conduct. To be the proximate cause is not necessarily to be the sole cause. OPM was the proximate cause of the harm befalling Arnold Plaintiffs so long as its conduct created a foreseeable risk of harm through the hackers' intervention.

The complaint alleges facts demonstrating proximate cause. Arnold Plaintiffs contend that OPM's failure to establish appropriate information security safeguards opened the door to the hackers, giving them ready access to a storehouse of personally identifiable and sensitive financial information. In particular, the complaint explains that OPM's failure to adopt basic protective measures "foreseeably heightened the risk of a successful intrusion into OPM's systems."

Numerous Arnold Plaintiffs suffered forms of identity theft accomplishable only with the type of information that OPM stored and the hackers accessed. That directly links the hack to the theft of the victims' private information, the pecuniary harms suffered, and the ongoing increased susceptibility to identity theft or financial injury. To argue, as OPM does, that the presumed occurrence of other data breaches defeats a causal connection as a matter of law at this early stage again wrongly construes inferences drawn from generic assertions about the general risk of data breaches in the government's favor. The law would embody quite a "perverse incentive" were it to hold at this threshold stage of litigation that, "so long as enough data breaches take place," agencies "will never be found liable."

In sum, we reverse in part and affirm in part. We hold that (i) . . . Arnold Plaintiffs have adequately alleged Article III standing; (ii) Arnold Plaintiffs have stated a claim under the Privacy Act, which waives OPM's sovereign immunity; [and] (iii) KeyPoint is not protected by derivative sovereign immunity . . . . We remand for further proceedings consistent with this opinion.

Notes

1. The OPM data breach hits on all the major questions under the Privacy Act. We have mens rea, actual harm, and even causation. The lawsuit also posed a number of questions not reviewed here, notably standing and the constitutional right to information privacy.

VII. Health Privacy

A. Common law roots of medical privacy 343
1) Duty of Confidentiality 344
Lawson v. Halpern-Reiss, 212 A.3d 1213 (2019) 344
2) Evidentiary Privileges 348
Jaffee v. Redmond, 518 U.S. 1 (1996) 348
3) Duty to Warn 354
Tarasoff v. Regents of University of California, 551 P.2d 334 (Cal. 1976) 354

B. The rise of HIPAA 359
1) The Privacy, Security, and Data Breach Rules 360
a) Limitations on the use and disclosure of PHI under the Privacy Rule 361
b) Data security requirements under the Security Rule 364
c) Data breach notification 365
2) State Medical Privacy Law as a Supplement to HIPAA 366
Shepherd v. Costco Wholesale Corporation, 482 P.3d 390 (Ariz. 2021) 368
3) HIPAA Civil Enforcement 371
Premera Blue Cross Resolution Agreement (2020) 373
Athens Orthopedic Clinic Resolution Agreement (2020) 375
Yakima Valley Memorial Hospital Press Release (2023) 377
4) HIPAA Criminal Enforcement 379
U.S. v. Huping Zhou, 678 F.3d 1110 (2012) 379

C. Privacy in genetic information 382
1) Use of genetic information for identification 382
Maryland v. King, 569 U.S. 435 (2013) 382
2) Use of genetic information for prediction 390

In general, health data receives a greater level of privacy protection than other data. One might think that this means that there is a single statute that regulates all of medical privacy, or that health information is uniformly regulated across the country. This is sadly not so. Medical privacy is regulated by three overlapping legal regimes: state common law, state statutory law, and federal law. The most famous regulation is the federal Health Insurance Portability and Accountability Act (HIPAA). But, as we shall see, medical privacy neither began nor ends with that statute.

This chapter begins by reviewing the common law roots of medical privacy, focusing on the duty of confidentiality, evidentiary privileges, and the limitations of both. Then it turns to federal regulation of medical privacy, examining the contours of HIPAA, and state law efforts to supplement it. Finally, it will consider genetic privacy.

The reason for this odd structure—state, then federal, then state—is that it is roughly chronological in nature. Medical privacy law began in the common law. Then it "went federal" with HIPAA in the 1990s. And then state medical privacy law grew substantial teeth as a way to supplement and fill gaps created by HIPAA. A decade ago, state medical privacy law would need not trouble students of privacy. That is no longer the case.

A. Common law roots of medical privacy

It is traditional to begin discussions of medical privacy with this excerpt from the Hippocratic Oath:

> Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private.

The musings of Greek philosophers are an imperfect guide to American common law, but for medical privacy they are not a bad start. Doctors work under a professional and legal duty of confidentiality in the majority of states. The below case is a testament to both the commonality of that duty and also its complexity. The general tension here is between protecting the privacy of the individual and the safeguarding of that individual, other individuals, and society at large.

1) Duty of Confidentiality

Lawson v. Halpern-Reiss, 212 A.3d 1213 (2019)

EATON, J.

In this appeal, we are asked to recognize a common-law private right of action for damages resulting from the unjustified disclosure to a third party of information obtained by medical personnel during treatment. Plaintiff [Lawson] alleges in her lawsuit that she incurred damages as the result of an emergency room nurse informing a police officer that she was intoxicated, had driven to the hospital, and was intending to drive home. The trial court granted defendant Central Vermont Medical Center (CVMC) summary judgment based on its determination that nothing in the record supported an inference that the nurse's disclosure of the information was for any reason other than her good-faith concern for plaintiff's and the public's safety. In this opinion, we recognize a common-law private right of action for damages based on a medical provider's unjustified disclosure to third persons of information obtained during treatment. Like the trial court, however, we conclude that CVMC was entitled to judgment as a matter of law because, viewing the material facts most favorably to plaintiff and applying the relevant law we adopt today, we conclude that no reasonable factfinder could determine that the disclosure was for any purpose other than to mitigate the threat of imminent and serious harm to plaintiff and the public. Accordingly, we affirm the trial court's judgment.

I. Facts and Procedural History

The following facts are taken from the parties' statements of undisputed material facts, viewing them most favorably to plaintiff, the nonmoving party. During the early morning hours of May 10, 2014, plaintiff drove herself to CVMC after lacerating her arm. She arrived at the emergency room at 2:12 a.m. The charge nurse (Clinical Nurse Coordinator) detected a heavy odor of alcohol on plaintiff's breath, and it became apparent to the nurse that plaintiff had been drinking. Members of the treatment team administered an alco-sensor test to assess plaintiff's level of intoxication. The test revealed a breath-alcohol concentration of .215, over two and one-half times the legal limit, at 2:40 a.m.

Based on information provided by plaintiff, the charge nurse understood that plaintiff did not have a ride home. After her laceration was treated, plaintiff did not meet the criteria for admission to the hospital and was cleared for discharge. She was discharged at 3:05 a.m.

A police officer was on duty in the emergency room pursuant to a contract between CVMC and the Berlin Police Department. Shortly before plaintiff was discharged, the charge nurse approached the officer and informed him that plaintiff was blatantly intoxicated, that she had driven herself to the hospital, and that she was about to drive herself home. After receiving this information from the charge nurse and communicating with plaintiff, the officer arrested her on suspicion of driving while intoxicated. The resulting criminal charge was later dismissed by the prosecutor.

In July 2016, plaintiff filed a complaint against the charge nurse and CVMC, alleging that she incurred damages as the result of (1) the nurse's negligent disclosure of information obtained during plaintiff's medical treatment, in violation of the standard of care applicable to medical providers; and (2) CVMC's inadequate training and failure to develop policies regarding the disclosure of information obtained during medical treatment.

In May 2018, the trial court granted summary judgment to CVMC.

II. The Claims of Error

On appeal, plaintiff argues that: (1) the trial court erred in holding that there is no common-law remedy for a health care provider's breach of a duty of confidentiality; and (2) assuming there is such a remedy, the court erred in granting CVMC summary judgment insofar as there are material facts in dispute as to whether the nurse breached the duty of confidentiality regarding information obtained during the course of medical treatment.

A. Private Right of Action

Plaintiff first argues that this Court should recognize a common-law private remedy for breach of a medical provider's duty of confidentiality concerning the disclosure of information obtained during medical treatment. Plaintiff seeks a common-law remedy because neither Vermont law nor HIPAA provides a private right of action to obtain damages incurred as the result of a medical provider's disclosure of information obtained during treatment.

English common law did not afford patients a cause of action based on an expectation of privacy in information disclosed during medical treatment, but the notion "that physicians should respect the confidences revealed by their patients in the course of treatment is a concept that has its genesis in the Hippocratic Oath." *McCormick v. England* (S.C. Ct. App. 1997). By the 1960s and 1970s, several courts had recognized a private right of action for damages resulting from medical providers' wrongful disclosure of information obtained during treatment, and currently the vast majority of jurisdictions addressing whether to recognize such a cause of action have chosen to do so.

In recognizing this common-law private right of action, courts have relied on various theories, "including invasion of privacy, breach of implied contract, medical malpractice, and breach of a fiduciary duty or a duty of confidentiality." The most commonly accepted theory is breach of the duty of confidentiality, insofar as "health care providers enjoy a special fiduciary relationship with their patients" such that "recognition of the privilege is necessary to ensure that the bond remains."

As evidence of sound public policy underlying the recognition of liability for breach of the duty of confidentiality, courts have cited "(1) state physician licensing statutes, (2) evidentiary rules and privileged communication statutes which prohibit a physician from testifying in judicial proceedings; (3) common law principles of trust, and (4) the Hippocratic Oath and principles of medical ethics which proscribe the revelation of patient confidences." At the core of this reasoning is that when confidentiality between a medical provider and a patient is diminished in any way, it negatively impacts trustful communication between the two, which, in turn, degrades the medical provider's ability to render effective treatment.

For the same public policy reasons, we join the consensus of jurisdictions recognizing a common-law private right of action for damages arising from a medical provider's unauthorized disclosure of information obtained during treatment.

Many of this state's laws underscore Vermont's policy of protecting patient confidentiality by prohibiting the disclosure of patient information. Under Vermont law, hospital patients have "the right to expect that all communications and records pertaining to [their] care shall be treated as confidential." 18 V.S.A. § 1852(a)(7).

On the other hand, and equally as important, various Vermont statutes compel medical providers to disclose certain information to protect the public. *See, e.g.*, 13 V.S.A. § 3504(a)(3) (providing immunity from civil suit for health care provider making good-faith report of disease associated with weapons of mass destruction); *id.* § 4012(a) (requiring physician treating gunshot wound to report case to law enforcement); 18 V.S.A. §§ 1001, 1004, 1007, 1041, 1092–1093 (requiring medical providers to report information concerning patients diagnosed with or suspected of having communicable diseases dangerous to public health); 23 V.S.A. § 1203b(a) (requiring medical provider who is treating person in emergency room as result of motor vehicle accident to report to law enforcement blood-test result exceeding legal limit, notwithstanding any law or rule to contrary). By requiring disclosure under certain circumstances and in some cases providing immunity for the disclosure, statutes such as these implicitly acknowledge that medical providers have a general duty of confidentiality and that a violation of that duty may subject them to liability.

The most recent and explicit examples of the Legislature's recognition of medical providers' duty of confidentiality is its enactment of a law prohibiting the disclosure of "protected health information" by a "covered entity," as the terms are defined by federal regulations, "unless the disclosure is permitted under" HIPAA. 18 V.S.A. § 1881.

Although we ultimately uphold the trial court's grant of summary judgment in favor of CVMC in this case, we adopt a widely recognized common-law private right of action, using the HIPAA framework as a guide, rather than speculate as to whether or what right of action we would adopt in considering whether defendant is entitled to summary judgment.

B. Summary Judgment Ruling

In this case, relying on a regulatory HIPAA exception for good-faith disclosures to prevent serious and imminent threats to the safety of the public, the trial court granted summary judgment to CVMC based on its determination the record did not contain "any reasonable inference that [the charge nurse's] disclosure to the onsite police officer was for law enforcement purposes or any other reason than out of a good-faith concern for [plaintiff's] and the traveling public's safety."

Both the trial court and the parties focused on the HIPAA regulation permitting "disclosures to avert a serious threat to health or safety." 45 C.F.R. § 164.512(j). In relevant part, the regulation permits a "covered entity" to disclose "protected health information" as long as two conditions are met: the covered entity has a good-faith belief that the disclosure is "necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public," and the disclosure is "to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat." The regulation further provides that a covered entity disclosing information pursuant to this exception is "presumed to have acted in good faith with regard to a belief described in" the exception.

We conclude that this exception, including its good-faith component, provides an appropriate limit to obtaining damages for the disclosure of information obtained during medical treatment. While we recognize that due care must "be exercised in order to insure that only that information which is necessary to protect the potential victim is revealed," we must be cautious in requiring medical providers, particularly in emergency situations such as this, to parse too finely what information can or cannot be disclosed to protect individuals or the public in general from an imminent and serious threat of harm.

CVMC does not contest that it is a covered entity and that the information provided to the onsite police officer was protected health information. Nor does plaintiff contest that, assuming there was a threat justifying disclosure of the information, the police officer was a person reasonably able to prevent the threat. The point of contention is whether the record demonstrates, as a matter of law, that the nurse had a good-faith belief that all the information

provided to the officer was necessary to prevent a serious and imminent threat to the health or safety of plaintiff or the general public.

In answering this question, we first reexamine what the nurse told the officer. As stated above, the nurse indicated that plaintiff was blatantly intoxicated, that she had driven herself to the hospital, and that she was about to drive herself home. Given the record before us, if the nurse had told the officer only that plaintiff was blatantly intoxicated and was about to drive herself home, CVMC would surely be entitled to summary judgment. But we must also consider that the nurse also told the officer that the blatantly intoxicated plaintiff had driven herself to the hospital, thereby suggesting that plaintiff had committed a crime. In considering this particular statement, we recognize that the disclosure exception in § 164.512(j)(1)(i) is directed at preventing future conduct, in the sense that it allows disclosures based on a good-faith belief that doing so is necessary to prevent the threat of imminent and serious harm.[7]

Because we have adopted the standards in HIPAA as framing the contours and limits of a cause of action for breach of the duty not to disclose protected health information, to answer the pivotal question in this case we must determine how "good faith" is defined for purposes of § 164.512(j)(1), (4)—and, in particular, whether to apply a subjective or objective test. For the following reasons, we conclude that the applicable test in this case is a subjective one. That is, whether the nurse's motivation for disclosing the protected health care information was based solely on her belief that the disclosure was necessary to protect or lessen a serious and imminent threat to health or safety, or whether the nurse sought to satisfy some other purpose, even a well-intentioned one, apart from this narrow legal exception to her general duty of nondisclosure.

Applying the subjective standard, we conclude that plaintiff has not met her burden of production to rebut the applicable presumption of good faith.

[T]he presumption of good faith in HIPAA, § 164.512(j)(4), which we adopt for purposes of analyzing the common-law tort we recognize in this decision, shifts the burden to plaintiff to make some showing that the nurse's disclosure that plaintiff had driven to the hospital and was blatantly intoxicated was not made in good faith.

Although the burden of production is not a heavy one, plaintiff did not meet hers in this case. Nothing in the record suggests that the nurse supplied the information to the officer for any reason other than her good-faith belief that the information was necessary to prevent plaintiff from driving drunk from the hospital and endangering herself and the public. Plaintiff made no proffer suggesting that the nurse hoped inclusion of the arguably superfluous information about how plaintiff got to the hospital would lead to plaintiff's censure, arrest, or prosecution or that she had any ulterior motive beyond the permitted one.

Notes

1. This case is notable both for its highly traditional move—finding a private cause of action for breach of confidentiality—and also its more modern move—defining the scope of that duty in terms of HIPAA. As you will see below, a person cannot sue under HIPAA itself. But HIPAA can be used to establish a standard of care. Doctors *should* do X. Therefore, failure

[7] That is in contrast to the exception in § 164.512(j)(1)(ii), which allows, in most instances, the disclosure of limited types of information when there is a good-faith belief that the disclosure is necessary for law enforcement to identify or apprehend someone either because that person has escaped from custody or because an individual has admitted to participating "in a *violent crime* that the covered entity reasonably believes may have caused serious physical harm to the victim." (Emphasis added.) HIPAA regulations also contain a permitted disclosure exception for law-enforcement purposes, but that exception has several conditions, including that the disclosure is in compliance with legal process or required by law and that it constitutes evidence of a crime that occurred on the premises of the covered entity.

to do X is a breach of their legal duties. This is much like citing a state criminal statute in support of a tort intrusion-upon-seclusion claim. The legal violation is evidence that a breach of privacy is highly offensive to a reasonable person.

2. Consider the difficult and nuanced policy questions raised by a doctor's duty of confidentiality. Why is it that doctors can report gunshot wounds and auto accident blood-test results? Think through the social benefits of allowing such reporting and the reasons why courts and legislatures may be less concerned about encouraging disclosures in those cases.

There are two different forms of privacy protection offered to medical information and medical providers. One is a duty of confidentiality, which stops medical professionals from volunteering information about a person's medical conditions. Duties of confidentiality are common in the medical domain. The second form of privacy protection is an evidentiary privilege, which stops medical professionals from being compelled by courts to testify about information. Even in the privacy-protective domain of medical information, evidentiary privileges are rare.

2) Evidentiary Privileges

The *Jaffee* case creates a psychotherapist–patient privilege, bringing to the federal level a privilege that had, to varying degrees, been introduced in every state.

Jaffee v. Redmond, 518 U.S. 1 (1996)

Justice STEVENS delivered the opinion of the Court.

After a traumatic incident in which she shot and killed a man, a police officer received extensive counseling from a licensed clinical social worker. The question we address is whether statements the officer made to her therapist during the counseling sessions are protected from compelled disclosure in a federal civil action brought by the family of the deceased. Stated otherwise, the question is whether it is appropriate for federal courts to recognize a "psychotherapist privilege" under Rule 501 of the Federal Rules of Evidence.

I

Petitioner is the administrator of the estate of Ricky Allen. Respondents are Mary Lu Redmond, a former police officer, and the Village of Hoffman Estates, Illinois, her employer during the time that she served on the police force. Petitioner commenced this action against respondents after Redmond shot and killed Allen while on patrol duty.

On June 27, 1991, Redmond was the first officer to respond to a "fight in progress" call at an apartment complex. As she arrived at the scene, two of Allen's sisters ran toward her squad car, waving their arms and shouting that there had been a stabbing in one of the apartments. Redmond testified at trial that she relayed this information to her dispatcher and requested an ambulance. She then exited her car and walked toward the apartment building. Before Redmond reached the building, several men ran out, one waving a pipe. When the men ignored her order to get on the ground, Redmond drew her service revolver. Two other men then burst out of the building, one, Ricky Allen, chasing the other. According to Redmond, Allen was brandishing a butcher knife and disregarded her repeated commands to drop the weapon. Redmond shot Allen when she believed he was about to stab the man he was chasing. Allen died at the scene. Redmond testified that before other officers arrived to provide support, "people came pouring out of the buildings," and a threatening confrontation between her and the crowd ensued.

Petitioner filed suit in Federal District Court alleging that Redmond had violated Allen's constitutional rights by using excessive force during the encounter at the apartment complex.

At trial, petitioner presented testimony from members of Allen's family that conflicted with Redmond's version of the incident in several important respects. They testified, for example, that Redmond drew her gun before exiting her squad car and that Allen was unarmed when he emerged from the apartment building.

During pretrial discovery petitioner learned that after the shooting Redmond had participated in about 50 counseling sessions with Karen Beyer, a clinical social worker licensed by the State of Illinois and employed at that time by the Village of Hoffman Estates. Petitioner sought access to Beyer's notes concerning the sessions for use in cross-examining Redmond. Respondents vigorously resisted the discovery. They asserted that the contents of the conversations between Beyer and Redmond were protected against involuntary disclosure by a psychotherapist-patient privilege. The district judge rejected this argument. Neither Beyer nor Redmond, however, complied with his order to disclose the contents of Beyer's notes. At depositions and on the witness stand both either refused to answer certain questions or professed an inability to recall details of their conversations.

In his instructions at the end of the trial, the judge advised the jury that the refusal to turn over Beyer's notes had no "legal justification" and that the jury could therefore presume that the contents of the notes would have been unfavorable to respondents. The jury awarded petitioner $45,000 on the federal claim and $500,000 on her state-law claim.

The Court of Appeals for the Seventh Circuit reversed and remanded for a new trial. Addressing the issue for the first time, the court concluded that "reason and experience," the touchstones for acceptance of a privilege under Rule 501 of the Federal Rules of Evidence, compelled recognition of a psychotherapist-patient privilege. "Reason tells us that psychotherapists and patients share a unique relationship, in which the ability to communicate freely without the fear of public disclosure is the key to successful treatment." As to experience, the court observed that all 50 States have adopted some form of the psychotherapist-patient privilege. The court attached particular significance to the fact that Illinois law expressly extends such a privilege to social workers like Karen Beyer.

II

Rule 501 of the Federal Rules of Evidence authorizes federal courts to define new privileges by interpreting "common law principles . . . in the light of reason and experience." The authors of the Rule borrowed this phrase from our opinion in *Wolfle v. United States* (1934), which in turn referred to the oft-repeated observation that "the common law is not immutable but flexible, and by its own principles adapts itself to varying conditions."

The common-law principles underlying the recognition of testimonial privileges can be stated simply. "'For more than three centuries it has now been recognized as a fundamental maxim that the public ... has a right to every man's evidence. When we come to examine the various claims of exemption, we start with the primary assumption that there is a general duty to give what testimony one is capable of giving, and that any exemptions which may exist are distinctly exceptional, being so many derogations from a positive general rule.'" *United States v. Bryan* (1950).

Guided by these principles, the question we address today is whether a privilege protecting confidential communications between a psychotherapist and her patient "promotes sufficiently important interests to outweigh the need for probative evidence . . . ." Both "reason and experience" persuade us that it does.

III

Like the spousal and attorney-client privileges, the psychotherapist-patient privilege is "rooted in the imperative need for confidence and trust." Treatment by a physician for physical ailments can often proceed successfully on the basis of a physical examination, objective information supplied by the patient, and the results of diagnostic tests. Effective psychotherapy,

by contrast, depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears. Because of the sensitive nature of the problems for which individuals consult psychotherapists, disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason, the mere possibility of disclosure may impede development of the confidential relationship necessary for successful treatment. As the Judicial Conference Advisory Committee observed in 1972 when it recommended that Congress recognize a psychotherapist privilege as part of the Proposed Federal Rules of Evidence, a psychiatrist's ability to help her patients

> "'is completely dependent upon [the patients'] willingness and ability to talk freely. This makes it difficult if not impossible for [a psychiatrist] to function without being able to assure . . . patients of confidentiality and, indeed, privileged communication. Where there may be exceptions to this general rule . . ., there is wide agreement that confidentiality is a *sine qua non* for successful psychiatric treatment.'"

By protecting confidential communications between a psychotherapist and her patient from involuntary disclosure, the proposed privilege thus serves important private interests.

Our cases make clear that an asserted privilege must also "serv[e] public ends." Thus, the purpose of the attorney-client privilege is to "encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice." And the spousal privilege, as modified in *Trammel v. United States* (1980), is justified because it "furthers the important public interest in marital harmony." The psychotherapist privilege serves the public interest by facilitating the provision of appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance.[10]

In contrast to the significant public and private interests supporting recognition of the privilege, the likely evidentiary benefit that would result from the denial of the privilege is modest. If the privilege were rejected, confidential conversations between psychotherapists and their patients would surely be chilled, particularly when it is obvious that the circumstances that give rise to the need for treatment will probably result in litigation. Without a privilege, much of the desirable evidence to which litigants such as petitioner seek access—for example, admissions against interest by a party—is unlikely to come into being. This unspoken "evidence" will therefore serve no greater truth-seeking function than if it had been spoken and privileged.

That it is appropriate for the federal courts to recognize a psychotherapist privilege under Rule 501 is confirmed by the fact that all 50 States and the District of Columbia have enacted into law some form of psychotherapist privilege. We have previously observed that the policy decisions of the States bear on the question whether federal courts should recognize a new privilege or amend the coverage of an existing one.[13]

---

[10] This case amply demonstrates the importance of allowing individuals to receive confidential counseling. Police officers engaged in the dangerous and difficult tasks associated with protecting the safety of our communities not only confront the risk of physical harm but also face stressful circumstances that may give rise to anxiety, depression, fear, or anger. The entire community may suffer if police officers are not able to receive effective counseling and treatment after traumatic incidents, either because trained officers leave the profession prematurely or because those in need of treatment remain on the job.

[13] Petitioner acknowledges that all 50 state legislatures favor a psychotherapist privilege. She nevertheless discounts the relevance of the state privilege statutes by pointing to divergence among the States concerning the types of therapy relationships protected and the exceptions recognized. A small

IV

All agree that a psychotherapist privilege covers confidential communications made to licensed psychiatrists and psychologists. We have no hesitation in concluding in this case that the federal privilege should also extend to confidential communications made to licensed social workers in the course of psychotherapy. The reasons for recognizing a privilege for treatment by psychiatrists and psychologists apply with equal force to treatment by a clinical social worker such as Karen Beyer. Today, social workers provide a significant amount of mental health treatment. Their clients often include the poor and those of modest means who could not afford the assistance of a psychiatrist or psychologist, but whose counseling sessions serve the same public goals. Perhaps in recognition of these circumstances, the vast majority of States explicitly extend a testimonial privilege to licensed social workers. We therefore agree with the Court of Appeals that "[d]rawing a distinction between the counseling provided by costly psychotherapists and the counseling provided by more readily accessible social workers serves no discernible public purpose."

These considerations are all that is necessary for decision of this case. A rule that authorizes the recognition of new privileges on a case-by-case basis makes it appropriate to define the details of new privileges in a like manner. Because this is the first case in which we have recognized a psychotherapist privilege, it is neither necessary nor feasible to delineate its full contours in a way that would "govern all conceivable future questions in this area."[19]

Justice SCALIA, with whom THE CHIEF JUSTICE joins as to Part III, dissenting.

The Court has discussed at some length the benefit that will be purchased by creation of the evidentiary privilege in this case: the encouragement of psychoanalytic counseling. It has not mentioned the purchase price: occasional injustice. That is the cost of every rule which excludes reliable and probative evidence—or at least every one categorical enough to achieve its announced policy objective.

In the past, this Court has well understood that the particular value the courts are distinctively charged with preserving—justice—is severely harmed by contravention of "the fundamental principle that 'the public . . . has a right to every man's evidence.'" Testimonial privileges, it has said, "*are not lightly created nor expansively construed,* for they are in derogation of the search for truth." The Court today ignores this traditional judicial preference for the truth, and ends up creating a privilege that is new, vast, and ill defined. I respectfully dissent.

II

Effective psychotherapy undoubtedly is beneficial to individuals with mental problems, and surely serves some larger social interest in maintaining a mentally stable society. But merely mentioning these values does not answer the critical question: Are they of such importance, and is the contribution of psychotherapy to them so distinctive, and is the application of normal evidentiary rules so destructive to psychotherapy, as to justify making our federal courts occasional instruments of injustice? On that central question I find the Court's analysis insufficiently convincing to satisfy the high standard we have set for rules that "are in derogation of the search for truth."

---

number of state statutes, for example, grant the privilege only to psychiatrists and psychologists, while most apply the protection more broadly.

[19] Although it would be premature to speculate about most future developments in the federal psychotherapist privilege, we do not doubt that there are situations in which the privilege must give way, for example, if a serious threat of harm to the patient or to others can be averted only by means of a disclosure by the therapist.

When is it, one must wonder, that *the psychotherapist* came to play such an indispensable role in the maintenance of the citizenry's mental health? For most of history, men and women have worked out their difficulties by talking to, *inter alios,* parents, siblings, best friends, and bartenders—none of whom was awarded a privilege against testifying in court. Ask the average citizen: Would your mental health be more significantly impaired by preventing you from seeing a psychotherapist, or by preventing you from getting advice from your mom? I have little doubt what the answer would be. Yet there is no mother-child privilege.

How likely is it that a person will be deterred from seeking psychological counseling, or from being completely truthful in the course of such counseling, because of fear of later disclosure in litigation? And even more pertinent to today's decision, to what extent will the evidentiary privilege reduce that deterrent? The Court does not try to answer the first of these questions; and it *cannot possibly have any notion* of what the answer is to the second, since that depends entirely upon the scope of the privilege, which the Court amazingly finds it "neither necessary nor feasible to delineate." If, for example, the psychotherapist can give the patient no more assurance than "A court will not be able to make me disclose what you tell me, unless you tell me about a harmful act," I doubt whether there would be much benefit from the privilege at all. That is not a fanciful example, at least with respect to extension of the psychotherapist privilege to social workers.

Even where it is certain that absence of the psychotherapist privilege will inhibit disclosure of the information, it is not clear to me that that is an unacceptable state of affairs. Let us assume the very worst in the circumstances of the present case: that to be truthful about what was troubling her, the police officer who sought counseling would have to confess that she shot without reason, and wounded an innocent man. If (again to assume the worst) such an act constituted the crime of negligent wounding under Illinois law, the officer would of course have the absolute right not to admit that she shot without reason in criminal court. But I see no reason why she should be enabled *both* not to admit it in criminal court (as a good citizen should), *and* to get the benefits of psychotherapy by admitting it to a therapist who cannot tell anyone else. And even less reason why she should be enabled to *deny* her guilt in the criminal trial—or in a civil trial for negligence—while yet obtaining the benefits of psychotherapy by confessing guilt to a social worker who cannot testify. It seems to me entirely fair to say that if she wishes the benefits of telling the truth she must also accept the adverse consequences. To be sure, in most cases the statements to the psychotherapist will be only marginally relevant, and one of the purposes of the privilege (though not one relied upon by the Court) may be simply to spare patients needless intrusion upon their privacy, and to spare psychotherapists needless expenditure of their time in deposition and trial. But surely this can be achieved by means short of excluding even evidence that is of the most direct and conclusive effect.

The Court confidently asserts that not much truth-finding capacity would be destroyed by the privilege anyway, since "[w]ithout a privilege, much of the desirable evidence to which litigants such as petitioner seek access . . . is unlikely to come into being." If that is so, how come psychotherapy got to be a thriving practice before the "psychotherapist privilege" was invented? Were the patients paying money to lie to their analysts all those years?

III

Turning from the general question that was not involved in this case to the specific one that is: The Court's conclusion that a social-worker psychotherapeutic privilege deserves recognition is even less persuasive. In approaching this question, the fact that five of the state legislatures that have seen fit to enact "some form" of psychotherapist privilege have elected not to extend *any form* of privilege to social workers ought to give one pause. So should the fact that the Judicial Conference Advisory Committee was similarly discriminating in its conferral of the proposed Rule 504 privilege. The Court, however, has "no hesitation in concluding . . . that the federal privilege should also extend" to social workers.

Of course this brief analysis—like the earlier, more extensive, discussion of the general psychotherapist privilege—contains no explanation of why the psychotherapy provided by social workers is a public good of such transcendent importance as to be purchased at the price of occasional injustice. Moreover, it considers only the respects in which social workers providing therapeutic services are *similar* to licensed psychiatrists and psychologists; not a word about the respects in which they are different. A licensed psychiatrist or psychologist is an expert in psychotherapy—and that may suffice (though I think it not so clear that this Court should make the judgment) to justify the use of extraordinary means to encourage counseling with him, as opposed to counseling with one's rabbi, minister, family, or friends. One must presume that a social worker does *not* bring this greatly heightened degree of skill to bear, which is alone a reason for not encouraging that consultation as generously. Does a social worker bring to bear at least a significantly heightened degree of skill—more than a minister or rabbi, for example? I have no idea, and neither does the Court. The social worker in the present case, Karen Beyer, was a "licensed clinical social worker" a job title whose training requirements consist of a "master's degree in social work from an approved program," and "3,000 hours of satisfactory, supervised clinical professional experience." It is not clear that the degree in social work requires *any* training in psychotherapy. The "clinical professional experience" apparently will impart some such training, but only of the vaguest sort, judging from the Illinois Code's definition of "[c]linical social work practice," viz., "the providing of mental health services for the evaluation, treatment, and prevention of mental and emotional disorders in individuals, families and groups based on knowledge and theory of psychosocial development, behavior, psychopathology, unconscious motivation, interpersonal relationships, and environmental stress." With due respect, it does not seem to me that any of this training is comparable in its rigor (or indeed in the precision of its subject) to the training of the other experts (lawyers) to whom this Court has accorded a privilege, or even of the experts (psychiatrists and psychologists) to whom the Advisory Committee and this Court proposed extension of a privilege in 1972.

Notes

1. A person does not waive psychotherapist privilege merely by telling people or a court that they are receiving therapy, or even by claiming particular diagnoses or prescriptions for medications. *United States v. Portillo*, 969 F.3d 144, 182 (5th Cir. 2020).
2. State courts do not always grant the same expansive protections to psychotherapist–patient communications as did *Jaffee*. For instance, an Alaska appellate court granted the defense review of mental health records in a criminal case. The court stated that "a defense request for *in camera* review of privileged mental health records should be granted if the defendant has shown a reasonable likelihood that the records will contain exculpatory evidence that is necessary to the defense and unavailable from a less intrusive source." *Douglas v. State*, 527 P.3d 291, 308 (Alaska Ct. App. 2023). It distinguished *Jaffee* on the grounds that *Jaffee* was civil rather than criminal and that here it was the defense, rather than plaintiff or prosecution, seeking records. In effect, the court was creating a balancing test; recognizing privacy but not fully granting it when the defense's constitutional interests are strong enough. What is better? The categorical rule in *Jaffee* or this balancing-of-interests approach?
3. Courts have generally rejected a "dangerous patient" exception to psychotherapist privilege. "Arising from this dictum is a "dangerous patient" exception to the psychotherapist-patient privilege discussed, but often rejected, by circuit courts." *United States v. Ghane*, 673 F.3d 771, 784 (8th Cir. 2012). This does not mean that a therapist can never testify without a waiver of the privilege, however. A therapist can testify at a patient's involuntary commitment proceeding, for instance, as that is consistent with the therapist's duty to protect the patient and innocent third parties. But this is different than testifying at the patient's criminal trial. *Id.* at 785–86.

4. Psychotherapist privilege is more common than physician–patient privilege. For instance, there is not a physician–patient privilege under federal law, and its status is highly variable at the state level. Many states recognize such a privilege in civil suits with exceptions. *See, e.g.*, VA. CODE § 8.01-399 (physician–patient privilege in civil actions except when "the physical or mental condition of the patient is at issue."). But some explicitly do not recognize such a privilege in criminal cases. *See, e.g.*, ALASKA R. EVID. 504 (recognizing a psychotherapist privilege in criminal cases but not a physician–patient privilege in criminal cases).
5. Privilege and confidentiality are often limited to information disclosed in appropriate circumstances. The communication must be made in the course of seeking medical treatment, in confidence, to a physician who is acting as a physician. A comment to a doctor or psychotherapist in a private office, as one is receiving treatment, and that is relevant to the treatment would generally fall within the duty. A comment to such a person in a public setting where others can easily hear, a comment irrelevant to the treatment, or a comment made without any expectation of privacy will not trigger a privilege.

3) Duty to Warn

Patients are protected from casual or malicious disclosures under a duty of confidentiality. They are protected against having their words and diagnoses used against them in court by evidentiary privileges, where applicable. But there is a rare case in which a therapist may be *required* to disclose patient information without their consent. Consider the case below.

Tarasoff v. Regents of University of California, 551 P.2d 334 (Cal. 1976)

TOBRINER, Justice.

On October 27, 1969, Prosenjit Poddar killed Tatiana Tarasoff. Plaintiffs, Tatiana's parents, allege that two months earlier Poddar confided his intention to kill Tatiana to Dr. Lawrence Moore, a psychologist employed by the Cowell Memorial Hospital at the University of California at Berkeley. They allege that on Moore's request, the campus police briefly detained Poddar, but released him when he appeared rational. They further claim that Dr. Harvey Powelson, Moore's superior, then directed that no further action be taken to detain Poddar. No one warned plaintiffs of Tatiana's peril.

Concluding that these facts set forth causes of action against neither therapists and policemen involved, nor against the Regents of the University of California as their employer, the superior court sustained defendants' demurrers to plaintiffs' second amended complaints without leave to amend.[2] This appeal ensued.

Plaintiffs' complaints predicate liability on two grounds: defendants' failure to warn plaintiffs of the impending danger and their failure to bring about Poddar's confinement pursuant to the Lanterman-Petris-Short Act. Defendants, in turn, assert that they owed no duty of reasonable care to Tatiana.

We shall explain that defendant therapists cannot escape liability merely because Tatiana herself was not their patient. When a therapist determines, or pursuant to the standards of his profession should determine, that his patient presents a serious danger of

[2] The therapist defendants include Dr. Moore, the psychologist who examined Poddar and decided that Poddar should be committed; Dr. Gold and Dr. Yandell, psychiatrists at Cowell Memorial Hospital who concurred in Moore's decision; and Dr. Powelson, chief of the department of psychiatry, who countermanded Moore's decision and directed that the staff take no action to confine Poddar. The police defendants include Officers Atkinson, Brownrigg and Halleran, who detained Poddar briefly but released him; Chief Beall, who received Moore's letter recommending that Poddar be confined; and Officer Teel, who, along with Officer Atkinson, received Moore's oral communication requesting detention of Poddar.

violence to another, he incurs an obligation to use reasonable care to protect the intended victim against such danger. The discharge of this duty may require the therapist to take one or more of various steps, depending upon the nature of the case. Thus it may call for him to warn the intended victim or others likely to apprise the victim of the danger, to notify the police, or to take whatever other steps are reasonably necessary under the circumstances.

In the case at bar, plaintiffs admit that defendant therapists notified the police, but argue on appeal that the therapists failed to exercise reasonable care to protect Tatiana in that they did not confine Poddar and did not warn Tatiana or others likely to apprise her of the danger.

Plaintiffs therefore can amend their complaints to allege that, regardless of the therapists' unsuccessful attempt to confine Poddar, since they knew that Poddar was at large and dangerous, their failure to warn Tatiana or others likely to apprise her of the danger constituted a breach of the therapists' duty to exercise reasonable care to protect Tatiana.

Plaintiffs' first cause of action, entitled 'Failure to Detain a Dangerous Patient,' alleges that on August 20, 1969, Poddar was a voluntary outpatient receiving therapy at Cowell Memorial Hospital. Poddar informed Moore, his therapist, that he was going to kill an unnamed girl, readily identifiable as Tatiana, when she returned home from spending the summer in Brazil. Moore, with the concurrence of Dr. Gold, who had initially examined Poddar, and Dr. Yandell, Assistant to the director of the department of psychiatry, decided that Poddar should be committed for observation in a mental hospital. Moore orally notified Officers Atkinson and Teel of the campus police that he would request commitment. He then sent a letter to Police Chief William Beall requesting the assistance of the police department in securing Poddar's confinement.

Officers Atkinson, Brownrigg, and Halleran took Poddar into custody, but, satisfied that Poddar was rational, released him on his promise to stay away from Tatiana. Powelson, director of the department of psychiatry at Cowell Memorial Hospital, then asked the police to return Moore's letter, directed that all copies of the letter and notes that Moore had taken as therapist be destroyed, and 'ordered no action to place Prosenjit Poddar in 72-hour treatment and evaluation facility.'

Plaintiffs' second cause of action, entitled 'Failure to Warn On a Dangerous Patient,' incorporates the allegations of the first cause of action, but adds the assertion that defendants negligently permitted Poddar to be released from police custody without 'notifying the parents of Tatiana Tarasoff that their daughter was in grave danger from Posenjit Poddar.' Roddar persuaded Tatiana's brother to share an apartment with him near Tatiana's residence; shortly after her return from Brazil, Poddar went to her residence and killed her.

The second cause of action can be amended to allege that Tatiana's death proximately resulted from defendants' negligent failure to warn Tatiana or others likely to apprise her of her danger. Plaintiffs contend that as amended, such allegations of negligence and proximate causation, with resulting damages, establish a cause of action. Defendants, however, contend that in the circumstances of the present case they owed no duty of care to Tatiana or her parents and that, in the absence of such duty, they were free to act in careless disregard of Tatiana's life and safety.

In analyzing this issue, we bear in mind that legal duties are not discoverable facts of nature, but merely conclusory expressions that, in cases of a particular type, liability should be imposed for damage done. 'The assertion that liability must . . . be denied because defendant bears no 'duty' to plaintiff 'begs the essential question—whether the plaintiff's interests are entitled to legal protection against the defendant's conduct. . . (Duty) is not sacrosanct in itself, but only an expression of the sum total of those considerations of policy which lead the law to say that the particular plaintiff is entitled to protection.' PROSSER ON THE LAW OF TORTS (3d ed. 1964).

The most important of these considerations in establishing duty is foreseeability. As a general principle, a 'defendant owes a duty of care to all persons who are foreseeably endangered by his conduct, with respect to all risks which make the conduct unreasonably dangerous.' As we shall explain, however, when the avoidance of foreseeable harm requires a defendant to control the conduct of another person, or to warn of such conduct, the common law has traditionally imposed liability only if the defendant bears some special relationship to the dangerous person or to the potential victim. Since the relationship between a therapist and his patient satisfies this requirement, we need not here decide whether foreseeability alone is sufficient to create a duty to exercise reasonably care to protect a potential victim of another's conduct.

Although plaintiffs' pleadings assert no special relation between Tatiana and defendant therapists, they establish as between Poddar and defendant therapists the special relation that arises between a patient and his doctor or psychotherapist. Such a relationship may support affirmative duties for the benefit of third persons. Thus, for example, a hospital must exercise reasonable care to control the behavior of a patient which may endanger other persons. A doctor must also warn a patient if the patient's condition or medication renders certain conduct, such as driving a car, dangerous to others.

Defendants contend, however, that imposition of a duty to exercise reasonable care to protect third persons is unworkable because therapists cannot accurately predict whether or not a patient will resort to violence. In support of this argument amicus representing the American Psychiatric Association and other professional societies cites numerous articles which indicate that therapists, in the present state of the art, are unable reliably to predict violent acts; their forecasts, amicus claims, tend consistently to overpredict violence, and indeed are more often wrong than right. Since predictions of violence are often erroneous, amicus concludes, the courts should not render rulings that predicate the liability of therapists upon the validity of such predictions.

We recognize the difficulty that a therapist encounters in attempting to forecast whether a patient presents a serious danger of violence. Obviously we do not require that the therapist, in making that determination, render a perfect performance; the therapist need only exercise 'that reasonable degree of skill, knowledge, and care ordinarily possessed and exercised by members of (that professional specialty) under similar circumstances.' Within the broad range of reasonable practice and treatment in which professional opinion and judgment may differ, the therapist is free to exercise his or her own best judgment without liability; proof, aided by hindsight, that he or she judged wrongly is insufficient to establish negligence.

In the instant case, however, the pleadings do not raise any question as to failure of defendant therapists to predict that Poddar presented a serious danger of violence. On the contrary, the present complaints allege that defendant therapists did in fact predict that Poddar would kill, but were negligent in failing to warn.

Amicus contends, however, that even when a therapist does in fact predict that a patient poses a serious danger of violence to others, the therapist should be absolved of any responsibility for failing to act to protect the potential victim. In our view, however, once a therapist does in fact determine, or under applicable professional standards reasonably should have determined, that a patient poses a serious danger of violence to others, he bears a duty to exercise reasonable care to protect the foreseeable victim of that danger. While the discharge of this duty of due care will necessarily vary with the facts of each case, in each instance the adequacy of the therapist's conduct must be measured against the traditional negligence standard of the rendition of reasonable care under the circumstances.

The risk that unnecessary warnings may be given is a reasonable price to pay for the lives of possible victims that may be saved. We would hesitate to hold that the therapist who is aware that his patient expects to attempt to assassinate the President of the United States

would not be obligated to warn the authorities because the therapist cannot predict with accuracy that his patient will commit the crime.

We recognize the public interest in supporting effective treatment of mental illness and in protecting the rights of patients to privacy and the consequent public importance of safeguarding the confidential character of psychotherapeutic communication. Against this interest, however, we must weigh the public interest in safety from violent assault. The Legislature has undertaken the difficult task of balancing the countervailing concerns. In Evidence Code § 1024, the Legislature created a specific and limited exception to the psychotherapist-patient privilege: 'There is no privilege . . . if the psychotherapist has reasonable cause to believe that the patient is in such mental or emotional condition as to be dangerous to himself or to the person or property of another and that disclosure of the communication is necessary to prevent the threatened danger.'

We realize that the open and confidential character of psychotherapeutic dialogue encourages patients to express threats of violence, few of which are ever executed. Certainly a therapist should not be encouraged routinely to reveal such threats; such disclosures could seriously disrupt the patient's relationship with his therapist and with the persons threatened. To the contrary, the therapist's obligations to his patient require that he not disclose a confidence unless such disclosure is necessary to avert danger to others, and even then that he do so discreetly, and in a fashion that would preserve the privacy of his patient to the fullest extent compatible with the prevention of the threatened danger.

Our current crowded and computerized society compels the interdependence of its members. In this risk-infested society we can hardly tolerate the further exposure to danger that would result from a concealed knowledge of the therapist that his patient was lethal. If the exercise of reasonable care to protect the threatened victim requires the therapist to warn the endangered party or those who can reasonably be expected to notify him, we see no sufficient societal interest that would protect and justify concealment. The containment of such risks lies in the public interest.

For the reasons stated, we conclude that plaintiffs can amend their complaints to state a cause of action against defendant therapists by asserting that the therapists in fact determined that Poddar presented a serious danger of violence to Tatiana, or pursuant to the standards of their profession should have so determined, but nevertheless failed to exercise reasonable care to protect her from that danger.

MOSK, Justice (concurring and dissenting).

I concur in the result in this instance only because the complaints allege that defendant therapists did in fact predict that Poddar would kill and were therefore negligent in failing to warn of that danger. Thus the issue here is very narrow: we are not concerned with whether the therapists, pursuant to the standards of their profession, 'should have' predicted potential violence; they allegedly did so in actuality. Under these limited circumstances I agree that a cause of action can be stated.

I cannot concur, however, in the majority's rule that a therapist may be held liable for failing to predict his patient's tendency to violence if other practitioners, pursuant to the 'standards of the profession,' would have done so.

I would restructure the rule designed by the majority to eliminate all reference to conformity to standards of the profession in predicting violence. If a psychiatrist does in fact predict violence, then a duty to warn arises. The majority's expansion of that rule will take us from the world of reality into the wonderland of clairvoyance.

CLARK, Justice (dissenting).

Until today's majority opinion, both legal and medical authorities have agreed that confidentiality is essential to effectively treat the mentally ill, and that imposing a duty on doctors to disclose patient threats to potential victims would greatly impair treatment. Further, recognizing that effective treatment and society's safety are necessarily intertwined, the Legislature has already decided effective and confidential treatment is preferred over imposition of a duty to warn.

The Legislature created a comprehensive statutory resolution of the rights and duties of both the mentally infirm and those charged with their care and treatment. Reflecting legislative recognition that disclosing confidences impairs effective treatment of the mentally ill, and thus is contrary to the best interests of society, the act establishes the therapist's duty to not disclose. Section 5328 provides in part that '(a)ll information and records obtained in the course of providing services . . . to either voluntary or involuntary recipients of services Shall be confidential.'

However, recognizing that some private and public interests must override the patient's, the Legislature established several limited exceptions to confidentiality. The limited nature of these exceptions and the legislative concern that disclosure might impair treatment, thereby harming both patient and society, are shown by section 5328.1. The section provides that a therapist may disclose 'to a member of the family of a patient the information that the patient is presently a patient in the facility or that the patient is seriously physically ill . . . if the professional person in charge of the facility determines that the release of such information is in the best interest of the patient.' Thus, disclosing even the fact of treatment is severely limited.

As originally enacted the act contained no provision allowing the therapist to warn anyone of a patient's threat. In 1970, however, the act was amended to permit disclosure in two limited circumstances. Section 5328 was amended, in subdivision (g), to allow disclosure '(t)o governmental law enforcement agencies as needed for the protection of federal and state elective constitutional officers and their families.' In addition, section 5328.3 was added to provide that when 'necessary for the protection of the patient or Others due to the patient's disappearance from, without prior notice to, a designated facility and his whereabouts is unknown, notice of such disappearance.' Obviously neither exception to the confidentiality requirement is applicable to the instant case.

The Legislature having determined that the balance of several interests requires nondisclosure in the graver public danger commitment, it would be anomalous for this court to reweigh the interests, requiring disclosure for those less dangerous.

Entirely apart from the statutory provisions, the same result must be reached upon considering both general tort principles and the public policies favoring effective treatment, reduction of violence, and justified commitment. Assurance of confidentiality is important for three reasons. [AUTH Note: to avoid deterring patients from treatment, promote full disclosure from patients, and facilitate successful treatment]

By imposing a duty to warn, the majority contributes to the danger to society of violence by the mentally ill and greatly increases the risk of civil commitment—the total deprivation of liberty—of those who should not be confined. The impairment of treatment and risk of improper commitment resulting from the new duty to warn will not be limited to a few patients but will extend to a large number of the mentally ill. Although under existing psychiatric procedures only a relatively few receiving treatment will ever present a risk of violence, the number making threats is huge, and it is the latter group—not just the former—whose treatment will be impaired and whose risk of commitment will be increased.

Notes

1. As of 2014, twenty-three states had a statutory mandatory reporting law in *Tarasoff*-like situations; ten had the duty at common law; and eleven had a permissive duty to warn, which immunizes practitioners from breach of confidentiality liability.[144] Yet these laws vary substantially by state, even within those categories. One key issue is whether the therapist in question needed to have actual knowledge of the threat to an identifiable victim or whether it is enough that they *should* have had such knowledge. For example, the post-*Tarasoff* California statute reads "[t]here shall be no monetary liability on the part of, and no cause of action shall arise against, any person who is a psychotherapist as defined in Section 1010 of the Evidence Code in failing to protect from a patient's threatened violent behavior or failing to predict and protect from a patient's violent behavior except if the patient has communicated to the psychotherapist a serious threat of physical violence against a reasonably identifiable victim or victims." CAL. CIV. CODE § 43.92 (2022). Consider how this statute relates to the concerns expressed in the Mosk concurrence/dissent above.
2. The *Tarasoff* rule is widely taught in counseling programs. One survey found that almost all responding psychiatry residency programs taught the duty to warn[145] and another that the overwhelming majority of clinical psychology programs did as well.[146] But that same survey of psychologists found that many misunderstood the threshold to trigger reporting in their particular state, which is perhaps somewhat fair given the legal uncertainty mentioned in note 1.
3. Despite the prevalence in education about *Tarasoff* duties, successful cases are rare. One analysis of appellate cases between 1985 and 2006 found seventy *Tarasoff*-type cases, with only six pro-plaintiff verdicts.[147]

B. The rise of HIPAA

A doctor's office in the early 1990s looked very different from one today. Back then, medical records were stored on paper, often consisting of handwritten notes that were difficult for anyone other than the original doctor to decipher. If a patient wanted to switch physicians, the new doctor needed a physical copy of the file. Since doctors were generally reluctant to lose patients, however, their offices often made obtaining these records cumbersome.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted in response to the transition from paper to electronic medical records. As records became digitized and standardized, concerns grew about unauthorized access to patient information (the "accountability" portion). At the same time, there was a recognized need to facilitate the transfer of medical records between providers (the "portability" portion). As today, a patient's choice of doctor was substantially a function of their health insurance, which was typically tied to their employer. Changing jobs meant needing to transfer medical records—a process that had to be both secure and efficient. But while portability was beneficial for patients seeking new care providers, it also introduced an enhanced risk of unauthorized access.

Consider a modern doctor visit. Your physician may not handle a single sheet of paper during the course of your appointment. Instead, they access your medical history digitally, not

---

[144] Rebecca Johnson, Govind Persad & Dominic Sisti, *The Tarasoff Rule: The Implications of Interstate Variation and Gaps in Professional Training*, 42 J. AM. ACAD. PSYCHIATRY L. 469 (2014).

[145] Mary Marrocco, Jonathan Uecker & Joseph Ciccone, *Teaching Forensic Psychiatry to Psychiatry* Residents, 23 BULL AM. ACAD. PSYCHIATRY L. 83 (1995).

[146] Yvona Pabian, Elizabeth Welfel & Ronald Beebe, *Psychologists' Knowledge of Their States' Laws Pertaining to Tarasoff-Type Situations*, 40 PRO. PSYCH.: RSCH. & PRAC. 8 (2009).

[147] Matthew Soulier, Andrea Maislen & James Beck, *Status of the Psychiatric Duty to Protect, Circa 2006*, 38 J. AM. ACAD. PSYCHIATRY L. 457 (2010).

only from their own records but potentially from other providers in their digital networks. And you may be able to view their notes and your test results online following this appointment. This connectivity offers tremendous convenience but also raises significant privacy concerns.

Finally, people often misspell HIPAA or assume that the "P" stands for privacy. It does not. Please be wary of these errors.

1) The Privacy, Security, and Data Breach Rules

By design, HIPAA is not a universal health privacy statute. It has a limited scope in that it only protects certain kinds of information created in certain contexts. It may be helpful to think of it as a *medical records* or *medical insurance* privacy statute rather than a *health* privacy statute.[148] What is protected is not your health information generally, but the information held by your doctors and their affiliates.

HIPAA's Privacy Rule concerns "protected health information" (PHI), which is defined as individually identifiable health information, including demographic information, that relates to:

- The individual's past, present, or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual.

This definition is intentionally broad. It also inherently does not include deidentified information. So, research facilities or marketing companies that use deidentified data are exempt from HIPAA enforcement.

There are no restrictions on the use or disclosure of deidentified health information. Deidentified health information is health information that neither identifies nor provides a reasonable basis to identify an individual. There are two ways to deidentify information; (1) a formal determination by a qualified statistician that the data alone, or in combination with other readily available information, could be used to reidentify the data; or (2) the removal of an extensive set of specified identifiers combined with the covered entity having no actual knowledge that the remaining information could be used to identify the individual.

HIPAA was intended to facilitate the creation of electronic medical records in "standard" formats that could then be intelligibly transferred between doctors and insurance providers. But this leads to one of the main limitations of HIPAA: it only applies to organizations that transmit information in a "standard" format created by the Department of Health and Human Services (HHS). In practice, everyone who takes insurance needs to transmit information in that format; it is how insurance and government benefit claims are processed. So, doctors, billing departments, and healthcare clearinghouses are all generally "covered entities." But HIPAA does not cover all medical information—only medical information held by entities like those and their business partners.

HIPAA therefore does not cover a range of entities in possession of health-related data. This includes fitness tracking apps, retailers who may profile people based on their purchases, and bars that ask if you are vaccinated. It also would not cover someone offering medical services who does not "transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard."[149] So a physical therapist who bills insurance would be a covered entity under HIPAA. A physical therapist who does not bill insurance but provides the same care is likely not a covered entity.

---

[148] Neither of these framings is perfect, so see which makes the most sense to you.

[149] For more details on covered entities, see https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

Many covered entities are part of broader organizations with missions that extend beyond medical care or whatever else makes them a covered entity. For example, a university might have a medical school that is a covered entity but also operate a law school and undergraduate campus that have little to do with the practice of medicine. Such an organization is called a "hybrid entity." Provided that the organization has sufficiently separated its parts, the portion of the hybrid entity engaged in health-care activities is covered by HIPAA and the remainder is not.

In addition to covered entities, HIPAA also regulates "business associates." These are companies that work with covered entities and need to access medical information from those entities. These could be billing companies, claim processers, medical transcriptionists, accounting firms, lawyers, and the like. For a covered entity to lawfully supply PHI to a business associate, it needs the associate to first execute a Business Associate Agreement. This document's purpose is to make sure the business associate is aware of its own obligations under HIPAA to limit access to and use of PHI and to ensure data security. When a covered entity becomes aware of a breach of this contract (or HIPAA generally) by a business associate, it has an obligation to report the problem and remedy the breach as best it can.

Covered entities are bound by HIPAA's Privacy, Security, and Data Breach Rules, described below. They also must give patients a statement of their privacy practices. The notice must describe the ways in which the covered entity may use and disclose PHI; state the covered entity's duties to protect privacy; describe individuals' rights, including the right to complain to HHS and to the covered entity if they believe their privacy rights have been violated; and include a point of contact for further information and for making complaints to the covered entity. Covered entities must act in accordance with their privacy notices.

HIPAA preempts state laws that are contrary to the HIPAA regulations. Contrary means that it would be impossible for a covered entity to comply with both the state and federal requirements, or that the provision of state law is an obstacle to accomplishing the full purposes and objectives of HIPAA. Adding to the privacy protections granted by HIPAA is generally permissible.

a) Limitations on the use and disclosure of PHI under the Privacy Rule

HIPAA's Privacy Rule governs the use and disclosure of PHI. A covered entity can only use or disclose information as permitted by the Privacy Rule or with the consent of the individual. With proper consent, a covered entity can make ambitious use of patient data. Without it, they cannot. There are few limitations placed on how consent can be obtained and what consent can do. Most basically, a covered entity cannot insist that a patient waive their rights under the Privacy Rule as a condition of receiving service.

HIPAA intends to give patients the right to decide with whom—apart from those necessarily involved in their care—their medical information is shared. But this process is not unthinking or blind to social convention. If a family member wishes to pick up a relative's prescription at a pharmacy, they will generally be able to do so. If a niece is going to drive her uncle home from the emergency room, she may be given basic instructions on his immediate care. Absent instructions to the contrary, medical professionals are allowed to use their professional judgment to communicate with family members. In effect, medical professionals can infer from social norms and circumstances what the patient's wishes might be.

When the patient objects, however, HIPAA does not permit sharing with family members outside special circumstances. If a person with a severe mental health condition has stopped taking their medications but remains competent to make medical decisions, a doctor cannot tell a family member of this choice unless the patient is a danger to themselves or others.

Covered entities can also disclose PHI to the individual it concerns. Occasionally a medical professional will cite HIPAA as a reason they cannot give a patient their own records. This is wrong except for a highly limited set of records.[150] In fact, HIPAA requires such information be provided and for it to be provided in a reasonable manner.[151]

Communication preferences. HIPAA requires covered entities to respect the reasonable communications preferences of patients. This is done so patients can determine for themselves whether they want a given health-care provider calling a shared phone number—perhaps a landline home phone or a work phone—or mailing reminder cards to a shared physical address.

Marketing. Marketing disclosures also require the consent of the individual. Given the big money to be made from medical marketing, this is a meaningfully important protection. Having said that, the definition of marketing excludes the covered entity's own services. So a spine surgeon can send advertisements for their in-house physical therapy clinic even without patient consent. Nor is it marketing for a health-care provider to send appointment reminders, reminders to make appointments, information about treatment and rehabilitation programs it runs, or anything else directly related to medical care. It is also not marketing when information is being shared for case-management purposes, for example with a nursing home who will be receiving a patient in the future. So all of these non-marketing communications and disclosures do not require consent.

Amendment. Patients have the right to request that their records be amended to correct what they believe are inaccuracies. These requests can be rejected but, if they are, it must be noted in the file that the request was made.

Complaints. Patients have the right to file a complaint either with the entity directly or via HHS without being retaliated against.

Minimum Necessary. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary requirement is not imposed when the disclosure is to a health-care provider for treatment; to an individual who is the subject of the information; made pursuant to an authorization; to HHS for complaint investigation; or required by law.

Disclosures Without Consent.

Even without consent, however, a covered entity may disclose PHI for a variety of reasons. A covered entity can disclose PHI for treatment purposes, including to another provider, and for the purposes of collecting payment or processing health-care claims. So a doctor's office can share PHI with another office in the process of referring a patient, for instance. Or they can compare notes to detect fraud or abuse if both offices have a relationship with the patient.

There are also a host of public-health and public-interest exceptions to HIPAA's Privacy Rule. Covered entities may disclose information to public-health authorities managing the spread of disease; to FDA-regulated authorities regarding adverse events, product recalls, and similar occurrences from drugs and medical devices; to people who may have been exposed to

---

[150] Specifically, psychotherapy notes, some internal payment processing information, and some information compiled for legal proceedings.

[151] A medical provider can charge a reasonable fee for doing so, but they cannot require requests be submitted by a single inconvenient method or impose other substantial obstacles. There are a host of explicit rules in this regard, but the basic principle is that they must give you the record.

communicable diseases (think HIV notification laws); and to employers when related to an on-the-job injury.[152]

Research. The Privacy Rule permits a covered entity to use and disclose PHI for research purposes, without an individual's authorization, provided the covered entity obtains either: (1) approval of the waiver of consent by an Institutional Review Board; (2) commitment from the researcher that the use or disclosure of the PHI is solely preparatory to research, that it is necessary for the research, and that it will not be removed from the covered entity; or (3) representations from the researcher that the use or disclosure sought is solely for research on the PHI of the deceased and is necessary. Also, recall that deidentified information is not PHI, meaning that it can be disclosed without consent.

Serious Threat to Health or Safety. Covered entities may disclose PHI they believe is "necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public," if the disclosure is "to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat." The regulation further provides that a covered entity disclosing information pursuant to this exception is "presumed to have acted in good faith with regard to a belief described in" the exception. For more on this, see the *Lawson* case, above.

Disclosures to Law Enforcement. Covered entities can disclose PHI to law enforcement under a variety of conditions. First, in the course of the serious health or safety exception above. Second, in response to a judicially authorized subpoena or warrant. Note that this does not impose a warrant requirement—a subpoena is sufficient.[153] Third, to respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness, or missing person. Fourth, to report child abuse or to make any other report required by state-specific law (gun shots, stab wounds, and the like). This exception will, depending on state law, sometimes authorize disclosures of adult abuse, elder abuse, and domestic violence without the consent of the victim. And, fifth, to report evidence of a crime that the covered entity believes occurred on its premises.

The Privacy Rule applies to all PHI and, for all PHI, it requires a covered entity to maintain reasonable administrative, technical, and physical safeguards to protect against intentional and unintentional disclosure of PHI in violation of the Privacy Rule. This would include shredding documents, training staff in privacy policies and procedures, and having reasonable building security.

Notes

1. The Privacy Rule revolves around consent, but is consent real in this context? For example, in 2024 NPR reported on how one provider of medical check-in software bundled targeted advertising with its program. During the appointment check-in process, patients were asked to give consent to having the contents of their medical files used for targeted advertising. This led to some patients believing that consent to advertising was linked to consent to receiving treatment. After complaints, the process was amended to make clear that consent to the advertising was both optional and separate from consent to treatment and the office's own privacy practices.[154] Presumably, however, there will be more of this in the future. Medical data and targeted medical advertising are lucrative.

---

[152] This last exception is related to the Worker's Compensation system.

[153] The amount of information to be disclosed would generally have to be limited in time and scope.

[154] Wailin Wong, Darian Woods, Julia Ritchey & Kate Concannon, *Ad Targeting Gets into Your Medical File,* NPR (Jan. 9, 2024), https://www.npr.org/2024/01/09/1197960899/ad-targeting-doctors-office-hipaa-data-privacy.

2. De-identification under HIPAA is not foolproof. In practice, HHS tolerates a small—though non-zero—risk of re-identification so that the difficulty of de-identification does not preclude valuable uses of the data. Notably, a 2010 HHS-commissioned study attempting to re-identify 15,000 safe-harbor records succeeded in matching only two individuals.[155] Other studies have shown more worrying results–especially when HIPAA de-identified data are combined with information that falls outside HIPAA. One study found that records involving motor-vehicle accidents could be re-identified by cross-referencing with publicly available data such as locations and manners of the accident.[156] Another study showed that combining physical activity data collected with wearable devices and machine learning techniques successfully re-identified a majority of supposedly de-identified HIPAA data.[157] Advances in artificial intelligence are compounding these challenges. Researchers have demonstrated that large language models can infer group membership from de-identified HIPAA clinical notes with notable accuracy.[158]
3. People often misunderstand HIPAA. Imagine a purse is stolen from a doctor's waiting room. Can the office staff identify the culprit, even using their own sign-in sheet to do so? Yes, that is expressly authorized by HIPAA. Can a doctor discuss a patient's treatment with the patient's spouse? Yes, if they believe in their professional judgment that this is what the patient wants. However, while HIPAA allows certain disclosures, it rarely mandates them. In the absence of a specific legal requirement to share information, healthcare providers are unlikely to face criticism for choosing not to disclose, even when disclosure is permitted.

b) Data security requirements under the Security Rule

The HIPAA Security Rule establishes national standards to protect individuals' *electronically stored* PHI (e-PHI) that is created, received, used, or maintained by a covered entity. So, while the Privacy Rule covers all PHI held by a covered entity, the Security Rule is limited to electronic data.

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated impermissible uses or disclosures; and
- Ensure compliance by their workforce.

These requirements are obviously not self-defining. And the Security Rule continues by stating that appropriate safeguards are also a function of the organization's size and

---

[155] Deborah Lafky, *The Safe Harbor Method of De-Identification: An Empirical Test (Dep't of Health & Hum. Servs., Oct. 8, 2009)*, https://www.ehcca.com/presentations/HIPAAWest4/lafky_2.pdf.

[156] Victor Janmey & Peter L. Elkin, *Re-Identification Risk in HIPAA De-Identified Datasets: The MVA Attack*, 2018 AMIA Annu. Symp. Proc. 1329 (Dec. 5, 2018), https://pmc.ncbi.nlm.nih.gov/articles/PMC6371259/.

[157] Liangyuan Na et al., *Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use of Machine Learning*, 1 JAMA Netw. Open e186040 (Dec. 21, 2018), https://doi.org/10.1001/jamanetworkopen.2018.6040.

[158] Atiquer Rahman Sarkar et al., *De-Identification Is Not Enough: A Comparison Between De-Identified and Synthetic Clinical Notes*, 14 Sci. Rep. 29669 (2024), https://doi.org/10.1038/s41598-024-81170-y.

capabilities, its hardware and software infrastructure, and a variety of other factors. Nevertheless, the Rule still has some rule-like requirements. An entity must:

- Conduct a risk analysis and management review, and this must be an ongoing process by which the organization considers how circumstances might have changed;
- Designate a security official to oversee the review and to implement necessary security programs;
- Have a system in place such that e-PHI is only accessible to those whose roles make such access reasonable;
- Train their entire workforce on security policies and procedures, and sanction those who violate them;
- Limit physical access to its facilities to authorized individuals;
- Secure workstations and electronic media—including in their disposal—so they cannot be accessed or obtained by unauthorized parties;
- Have audit controls, so they can determine who has accessed particular electronic files; and
- Transmit e-PHI only on secure networks.

Think about how this list of requirements impacts a practice. On one hand, they may sound intimidating if one pictures a solo-practitioner or small family practice. On the other, the burden of many of these requirements will scale with the size of the office. In a small practice, there will only be a few staff who need to undergo HIPAA training, and many vendors offer such programs. The most demanding of the electronic security requirements are also generally addressed by using HIPAA-compliant software, so HIPAA is not asking MDs to develop data-security expertise. In a large hospital, however, thousands of employees would need to undergo HIPAA training. Information will be shared in complex ways across departments. Many different categories of employees will exist, each requiring different access controls. Rather than the "security officer" being one of many roles held by an office manager, the security officer instead would need to have a staff. Rather than relying on vendors' claims about their software's HIPAA compliance, the security officer instead would need to investigate it for themselves.

c) Data breach notification

A data breach under HIPAA is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of *unencrypted* PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity demonstrates that there is a low probability that the information has been compromised.[159] Covered entities can also simply provide the data-breach notification and skip the risk assessment.

There are three exceptions to this broad definition of "breach." The first exception applies to the unintentional acquisition, access, or use of PHI by a workforce member or someone acting under the covered entity's authority, if such acquisition, access, or use was made in good faith and within the scope of authority. This covers a variety of basic workplace accidents, for example opening the wrong patient's file. The second exception applies to the inadvertent disclosure of PHI by one person authorized to access it to another person authorized to access it at the same entity. In both cases, the information cannot be further used or disclosed in a

[159] This assessment considers: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated.

manner not permitted by the Privacy Rule. The final exception applies if the covered entity or business associate has a good-faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

In the event of a breach, notification must be given to the affected individuals. This notice must be made without reasonable delay and in no case later than sixty days following the discovery of the breach. If the breach is large and affects more than 500 individuals, then the covered entity must notify both HHS and the media on the same timetable as the individuals themselves. If the breach is smaller than 500 people, the entity can make an annual report to HHS and need not notify the media. One consequence of this system is that HHS has a centralized database of all reported data breaches.

2) State Medical Privacy Law as a Supplement to HIPAA

In addition to the protections provided by HIPAA at the federal level and the common law at both the state and federal level, medical information can also be protected by state statutes. The basic rule is that states cannot decrease the amount of protection afforded by HIPAA, which sets the nationwide minimum. States can exceed that minimum, however, and several do. Most notable in this regard is the My Health My Data Act (MHMDA) from Washington state, which took effect on March 31, 2024.

There are three primary distinctions between the protections provided by HIPAA and by MHMDA. First, MHMDA covers a broader range of entities and data than does HIPAA. Specifically, it covers consumer health data (CHD) collected in Washington state by "regulated entities." The definition of 'regulated entity" is simply an entity that conducts business in Washington State and that "alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data."[160] HIPAA has nothing to say about medical information you give to Apple Health or Target. The MHMDA, on the other hand, regulates those. This is the first major distinction between the statutes.

Second, the definition of CHD is broader than the definition of PHI. CHD is defined as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present or future physical or mental health status." This includes data about health conditions and treatment, testing and diagnoses, biometric identifiers, genetic data, medical history, efforts to find information on reproductive health or gender-affirming care, precise location data that can reveal visits to health facilities, and the like. CHD also includes health inferences derived about consumers from non-health data, which is potentially quite broad.

Excluded from the definition of CHD are publicly available information and deidentified data, though biometric information collected from a consumer without their knowledge cannot be considered publicly available. Also, someone acting in an employment context is not a consumer under the Act, so employee data is not covered. There are also a variety of exceptions for data used for research, which somewhat mirror HIPAA's research exceptions, and exclusions for data that falls within the scope of HIPAA itself, the Gramm–Leach–Bliley Act, the Social Security Act, the Fair Credit Reporting Act, and the Family Educational Rights and Privacy Act.

Third, the Act provides greater protection than does HIPAA. It borrows from the list of protections found in laws like the California Consumer Privacy Act and Europe's General Data Protection Directive. Those familiar with those laws will find these rights familiar. Under the MHMDA, consumers have a right to access their CHD and receive a list of all third parties and affiliates who receive their individual data from the regulated entity. This transparency

[160] The definition excludes governmental entities, tribes, and contractors processing CHD on behalf of the government. Wash. Rev. Code. Ann. § 19.373.010(23).

obligation includes requiring entities to have a health-data privacy policy that describes what data is collected and how it is shared. Entities cannot collect, use, or share data for reasons outside the scope of the privacy policy. They cannot sell CHD without the consumer's consent. If an entity chooses to process health data, it must restrict access to the data to only those who require access for the purposes stated in the privacy policy. Washington consumers also have a right to withdraw their consent from an entity collecting and sharing their health data. If a consumer requests to have their health data deleted, the regulated entity must also delete it from archives and backups, and notify all affiliates and third parties, who must honor the deletion request as well.

Since the Act does not apply to HIPAA-covered data, these greater protections *only* apply to data *not* held by doctors, hospitals, and the like.

The MHMDA is enforceable both by the Washington Attorney General and by private parties under the Washington consumer protection statute. That statute does not provide for statutory damages for private suits, however, so the person would need to have some actual damages.

No other state has a law nearly as extensive as MHMDA. Though many states have medical-privacy laws, they often mirror HIPAA in every key respect. New York and Illinois, for instance, cover the same entities that HIPAA covers and provide basically the same protections. When statutes deviate from HIPAA, those deviations are often comparatively minor. Consider Illinois's Mental Health and Developmental Disabilities Confidentiality Act, which cross-references HIPAA's definitions of covered entities and business associates. It has enhanced consent obligations, requiring consent for the sharing of PHI to be in writing and include specific information about the purpose of the disclosure, the nature of the information being disclosed, and several other points. "Blanket consent" is specifically not valid. It only applies to certain kinds of mental-health data, however.

Notes

1. What are the drawbacks of MHMDA? Is it filling only obvious gaps left by HIPAA, or is it doing far more? How sweeping are its provisions from the standpoint of health-adjacent businesses, which previously needed to give little consideration to medical-privacy laws?
2. In one recent class action, the plaintiff alleged that Amazon's software development kits (SDKs), which are used by mobile application developers and run in the background of mobile applications, violated MHMDA by collecting users' location information and mobile advertising IDs. See *Maxwell v. Amazon.com, Inc.*, Case No. 2:25-cv-261 (W.D. Wash.). The plaintiff alleged Amazon failed to obtain consent or to disclose their collection, as required by MHMDA. They urge a broad interpretation of the "consumer health data" protected by the Act, asserting that location data "could reasonably indicate a consumer's attempt to acquire or receive health services or supplies." The court will have to determine whether such location data falls within the definition of CHD under the act.
   Some experts are skeptical of the MHMDA claim's liability theory: because Amazon only provided the SDKs, which were deployed by third-party developers, they may not be considered the collector of data.[161] The MHMDA does not recognize any aider-and-abettor theory of liability, so the court will have to rule on whether Amazon qualifies as a collector. It is common in privacy class actions to present many alternative theories of recovery. In this case, the MHMDA claim was bunded with more traditional privacy causes of action, including the Wiretap Act, the Stored Communications Act, and common law intrusion. In

[161] Starr Turner Drum & Alexander Altman, *Unpacking First Consumer Claim Under Wash. Health Data Act*, LAW360 (Mar. 14, 2025, 4:37 PM EDT), https://www.law360.com/compliance/articles/2310503/unpacking-first-consumer-claim-under-wash-health-data-act.

this way, the lawsuit is similar to some of the cookie and pixel litigation pursued against Google and Meta.

In addition to specific statutory laws adding to HIPAA's protection, state tort law sometimes provides an avenue for individuals to enforce their rights under HIPAA. This was seen in the *Lawson* case above, which concerned one set of HIPAA's exceptions. The below case concerns another.

Shepherd v. Costco Wholesale Corporation, 482 P.3d 390 (Ariz. 2021)

JUSTICE MONTGOMERY, opinion of the Court:

We are called upon in this case to determine what a plaintiff must allege for a claim of negligent disclosure of medical information to withstand a motion to dismiss based on the immunity provided by A.R.S. § 12-2296, and the extent to which the Health Insurance Portability and Accountability Act ("HIPAA") may be relied on for a claim of negligence.

Section 12-2296 affords healthcare providers immunity from liability for damages if they acted in good faith when disclosing medical information pursuant to applicable law. While acting in good faith is presumed, the presumption may be rebutted by clear and convincing evidence. We hold that a plaintiff does not have to allege bad faith or rebut the good faith presumption in his complaint when asserting a claim of negligent disclosure of medical information. We also hold that HIPAA may inform the standard of care in a negligence claim.

Greg Shepherd visited his physician for a check-up and a refill of his usual prescription. He also received a sample of an erectile dysfunction ("E.D.") medication. Thereafter, Shepherd went to Costco Pharmacy ("Costco") to pick up his regular prescription and was notified that a full prescription of the E.D. medication was ready, too. Shepherd said that he did not want the E.D. prescription and instructed the Costco employee to cancel it. The employee acknowledged the request.

Shepherd called Costco the next month to check on his regular prescription refill. An employee told him that the regular and E.D. prescriptions were ready. Shepherd again stated that he did not want the E.D. prescription and, again, his request was acknowledged.

Shepherd called back the next day, asking if his ex-wife, with whom he was exploring possible reconciliation, could pick up his regular prescription. The employee stated she could and that it was ready. The employee did not tell Shepherd, though, that the E.D. prescription was still available for pick up, as well.

When Shepherd's ex-wife went to Costco, the employee gave her both prescriptions. However, she did not accept the E.D. prescription, and the two joked about it. Upon returning to Shepherd, she told him she knew about the E.D. medication and no longer wanted to be with him, ending any reconciliation effort. She later told Shepherd's children and friends about the E.D. medication.

Shepherd complained to Costco headquarters about the disclosure of the E.D. prescription and received a written response acknowledging a violation of HIPAA and Costco's privacy policy. Shepherd then sued Costco, alleging negligence, breach of fiduciary duty, fraud, negligent misrepresentation, intentional infliction of emotional distress, intrusion upon seclusion, and public disclosure of private facts based on Costco's "public disclosure of an embarrassing medication that [he] twice rejected." Shepherd further alleged that had he known Costco failed to cancel the E.D. prescription, he would not have sent his ex-wife to pick up his regular prescription.

Costco argues that Shepherd's negligence claim should be dismissed as a matter of law given the qualified immunity provided by § 12-2296 and because HIPAA does not permit a private right of action. We address each argument in turn.

A. Qualified Immunity

Costco's main argument is that Shepherd's complaint fails to plead facts establishing bad faith by Costco. Therefore, he has failed to rebut the good faith presumption in § 12-2296, leaving Costco immune from his claim of negligence and requiring dismissal as a matter of law.

Because what constitutes good faith pursuant to § 12-2296 will arise on remand and the parties have briefed the issue, we proceed to define the term.

Section 12-2296 states:

> A health care provider . . . that acts in good faith under this article is not liable for damages in any civil action for the disclosure of . . . information contained in medical records . . . that is made pursuant to this article or as otherwise provided by law. The health care provider . . . is presumed to have acted in good faith. The presumption may be rebutted by clear and convincing evidence.

While several terms within § 12-2296 are defined elsewhere in article 7.1, good faith is not. The parties and courts below differ on the source for and substance of a definition of good faith.

Shepherd argues that a definition of good faith should have subjective and objective components similar to the UCC definition of good faith at A.R.S. § 47-8102(A)(10), which "for purposes of the obligation of good faith in the performance or enforcement of contracts or duties within this chapter, means honesty in fact and the observance of reasonable commercial standards of fair dealing." To underscore his point, he insists that a definition limiting good faith to "honesty in fact" is insufficient to provide protection for medical records privacy because that would only require "a pure heart and an empty head."

Costco, on the other hand, cites *Ramirez v. Health Partners of S. Ariz.* (Ariz. Ct. App. 1998) to define good faith. *Ramirez* observed that courts had consistently defined good faith under the Revised Uniform Anatomical Gift Act as an "honest belief, the absence of malice and the absence of a design to defraud or to seek an unconscionable advantage."

Between the UCC definition of good faith and the definition provided in *Ramirez*, we conclude that *Ramirez*'s definition is better suited for determining qualified immunity under § 12-2296. The UCC definition is necessarily concerned with the commercial nature of a transaction. Similarly, Shepherd's proffered definition is specifically focused on "good faith in the performance or enforcement of contracts or duties within this chapter," which addresses investment securities.

However, the disclosure of medical records addressed by § 12-2296 can occur outside of the context of a commercial transaction. For example, § 12-2294(C) discusses disclosure to a healthcare provider to provide diagnosis or treatment to a patient, to an ambulance attendant for transferring or providing services to a patient, to a legal representative to obtain legal advice, and to a patient's third party payor or contractor. Therefore, a definition that is focused on the conduct of a healthcare provider, regardless of the nature of the context in which the disclosure occurs, is more appropriate. We thus conclude that a healthcare provider acts in good faith where it acts under an honest belief, without malice or a design to defraud or to seek an unconscionable advantage.

C. HIPAA

Costco also argues that Shepherd's negligence claim fails as a matter of law because HIPAA does not provide for a private right of action. Therefore, it cannot support a negligence

per se claim or be used to establish the standard of care for negligence. Additionally, permitting a HIPAA cause of action undermines the immunity afforded by § 12-2296. For the following reasons, we disagree.

Costco is correct that HIPAA does not provide a private right of action. No court has held otherwise, and neither do we. But, as the court of appeals noted, HIPAA does not preclude state law tort claims. Other jurisdictions have reached the same conclusion, as well. While it is clear that HIPAA does not provide for a private right of action, it is equally clear that it does not prohibit a state law claim for negligent disclosure of medical information and thus does not preclude Shepherd's negligence claim.

Costco argues that Shepherd solely relies on HIPAA for his claim of negligence, which amounts to an impermissible negligence per se claim. However, in addition to HIPAA, the complaint references regulations governing pharmacies and Costco's privacy policy.

With respect to its privacy policy, Costco asserts that it cannot be used to establish the standard of care. While Costco is correct that a company's policies may not establish the standard of care, they may inform it. Costco's own citations prove the point. *See Quijano v. United States* (5th Cir. 2003) (concluding that under Texas law, "a hospital's internal policies and bylaws *may be evidence of the standard of care*," even though these rules alone cannot establish it (emphasis added)) . . . . Shepherd's reference to Costco's company policies thus provides an additional source to inform the standard of care beyond the sole provisions of HIPAA, as does his reference to regulations governing pharmacies.

To the extent Costco argues that *any* use of HIPAA to inform the standard of care in a negligence claim is precluded, we disagree. While some courts have concluded otherwise, we find the weight of authority permitting the use of HIPAA to inform the standard of care persuasive. We conclude that Shepherd permissibly referenced HIPAA in his complaint to inform the standard of care in his negligence claim. The trial court thus erred in granting Costco's motion to dismiss on this basis.

Costco further argues that permitting Shepherd to allege negligence with reference to HIPAA undermines the immunity afforded healthcare providers for good faith conduct under § 12-2296. We disagree. Shepherd must still rebut by clear and convincing evidence the statutory presumption that Costco acted in good faith. If he cannot, Costco will be immune from liability for damages due to any negligent disclosure of medical information.

III. Conclusion

Shepherd was not required to anticipate Costco's affirmative defense of qualified immunity under § 12-2296 in his complaint and allege bad faith, let alone allege clear and convincing evidence to rebut the good faith presumption. Shepherd also permissibly referenced HIPAA to inform the standard of care for his negligence claim. Consequently, we reverse the trial court's order granting Costco's motion to dismiss and remand for proceedings consistent with this opinion.

Notes

1. This case settled in 2022 on undisclosed terms. What do you think would be appropriate damages for a case like this? On one hand, there is no direct financial loss; Shepherd was not denied employment opportunities or physically injured. On the other, the exposure of his private information materially upset parts of his personal life. How would you frame the issue?
2. As with *Lawson* above, this case concerns a state-law claim that uses HIPAA to inform the standard of care. Think about Shepherd's experience through the lens of HIPAA. Is it reasonable for a pharmacist to allow a spouse to pick up a prescription? Presumably yes. What does it take to make it unreasonable to the point that good faith can be questioned?

3. Both here and in *Lawson* the medical practitioner is being granted a presumption of good faith. In *Lawson*, this was because HIPAA specifically granted such a presumption for dangerousness notifications. Here, it is because Arizona law granted a similar presumption of good faith more broadly. Does it make sense to grant such a presumption? Here, the court holds "that a healthcare provider acts in good faith where it acts under an honest belief, without malice or a design to defraud or to seek an unconscionable advantage." What portions of that definition are arguably disputed in this case?
4. Think about the last time you filled a prescription or picked up a prescription for someone else. In general, the pharmacist will ask for the name on the prescription and the date of birth of the person to whom it is prescribed. Rarely will the person picking up the prescription be asked to show ID. The experience is different if, for instance, the substance being prescribed is especially prone to abuse or if there is a note in the patient's file. But why does this seem to work well as a general rule? We do not have an epidemic of falsely picked-up prescriptions.

3) HIPAA Civil Enforcement

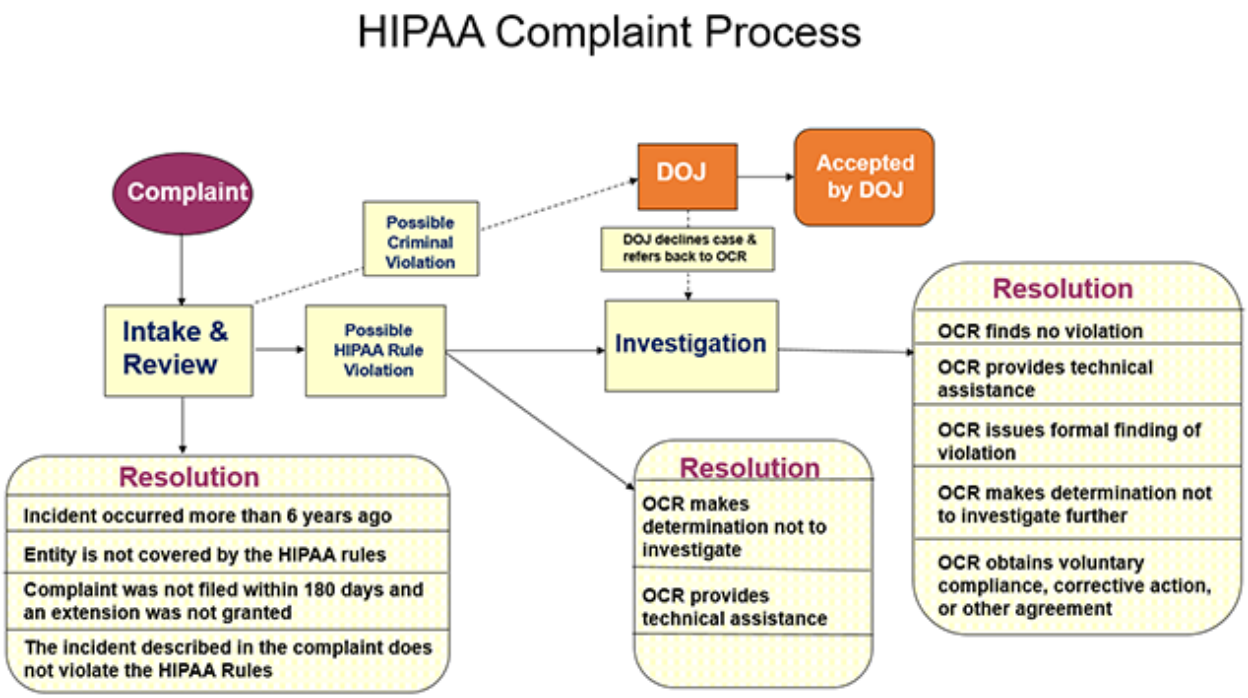
HIPAA is not directly enforced by individual private lawsuits. The statute contains no private right of action, and individuals only have the option of filing complaints with the HHS Office of Civil Rights (OCR). The total number of such complaints is fairly large. In 2021, there were 34,077 of them. This is an increase from prior years, though not a drastic one (27,182 in 2020 and 28,261 in 2019). These numbers are up substantially from the pre-2010 era, however, when there were approximately 8,000 complaints per year. The number of complaints only passed 15,000 in 2014.

OCR reviews all complaints that it receives. Under the law, OCR may take action only on complaints that meet the following conditions:

- The alleged action must have occurred in the past six years.
- The complaint must be filed against an entity that is required by law to follow the HIPAA Rules.
- The complaint must allege an activity that, if proven true, would violate HIPAA.
- Complaints must be filed within 180 days of when the person submitting the complaint knew or should have known about the alleged violation of the HIPAA Rules. OCR may waive this time limit if it determines that the person submitting the complaint shows good cause.

The below diagram shows the flow of the review process. Entities can face a penalty even if they were unaware of the regulations, which is why it is important for organizations to be aware of privacy laws. Note the possibility of a criminal referral to the Department of Justice. More on that later.

Between 2018 and 2021, 71.4% of complaints were resolved at the intake and review



stage.[162] 23.8% resulted in technical assistance to the accused party. A further 2.0% were found not to be violations. And, finally, 2.8% received corrective action.

Take 2021 as an example. 26,420 complaints were resolved. 20,661 (78.1%) were resolved after intake and review. A further 4,139 (15.7%) received pre-investigation technical assistance. 1,620 were investigated with a little less than half (714) resulting in corrective action; about half (817) resulting in a finding of no violation (817); and some (89) getting post-investigation technical assistance.

These numbers only refer to HIPAA complaints, however. There is a further set of HIPAA data breaches, reported to OCR under the HIPAA data-breach rule. There were 554 such reports in 2021, with 466 receiving corrective action.

The term corrective action is not synonymous with monetary penalty. Only fifty-three monetary settlements were filed across all four of the years from 2018 to 2021, meaning approximately thirteen settlements per year.

Still, what do these numbers tell us about HIPAA's enforcement? On one hand, the probability of a large fine under HIPAA appears vanishingly small. Part of this comes from the general orientation of HIPAA enforcement. The early years of HIPAA enforcement were focused on education—telling covered entities what they should do under the assumption that the entities would, in good faith, attempt to do it. This education focused approach still informs HIPAA enforcement today. And, while monetary penalties are rare, hospitals and doctors'

[162] Compliance statistics taken from the HHS website, which for some unclear reason has a large number of dead links: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html.

offices spend a great deal of time and energy thinking about HIPAA. Compliance with HIPAA is big business.

The most common types of HIPAA violations were relatively consistent across years:

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2021	Impermissible Uses & Disclosures	Access	Safeguards	Administrative Safeguards	Breach - Notice to Individual
2020	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Technical Safeguards
2019	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Minimum Necessary
2018	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards

The rarity of major financial penalties under HIPAA should not be mistaken for an absence of such. We do see major enforcement actions every year with six- or seven-figure penalties. These actions tend to fall into two categories: (1) large data breaches where the cybersecurity inadequacies of the covered entity led to the breach and (2) intentional access or release of patient data by insufficiently managed employees. As you read these enforcement actions, think back to the requirements of HIPAA's Security Rule.

Premera Blue Cross Resolution Agreement (2020)[163]

On March 17, 2015, PBC submitted a breach report indicating that it experienced a cyberattack beginning on May 5, 2014. The cyber-attackers gained impermissible access to the electronic protected health information (ePHI) of 10,466,692 individuals. The attackers initially gained unauthorized access to PBC's network through an email phishing campaign which installed malware on a system in the Premera network beginning on May 5, 2014 and went undetected until January 29, 2015. HHS's investigation indicated potential violations of the following provisions ("Covered Conduct"):

A. The requirement to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by PBC.

B. The requirement to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

C. Until March 8, 2015, the requirement to implement sufficient hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

D. The requirement to prevent unauthorized access to the ePHI of 10,466,692 individuals whose information was maintained in PBC's network.

Terms and Conditions

Payment. HHS has agreed to accept, and PBC has agreed to pay HHS, the amount of $6,850,000 ("Resolution Amount"). PBC agrees to pay the Resolution Amount on April 30, 2020, pursuant to written instructions to be provided by HHS.

[163] Full agreement at https://www.hhs.gov/sites/default/files/premera-ra-cap.pdf

Corrective Action Plan. PBC has entered into and agrees to comply with the Corrective Action Plan ("CAP").

PBC agrees to the following:

A. Conduct Risk Analysis

1. PBC shall conduct an accurate and thorough Risk Analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by PBC.

2. PBC shall provide the Risk Analysis . . . to HHS within ninety days of the Effective Date for HHS's review. HHS shall approve, or, if necessary, require revisions to PBC's Risk Analysis. The risk analysis shall include all ePHI created, received, maintained, or transmitted by PBC, and include but not be limited to, ePHI stored on or accessed by electronic information systems, networks, and applications administered or controlled by PBC. PBC may submit a Risk Analysis currently underway or previously completed within the past 180 days for consideration by HHS for compliance with this provision.

3. Within sixty days of its receipt of PBC's Risk Analysis, HHS will inform PBC in writing as to whether HHS approves the Risk Analysis or HHS requires revisions. If HHS requires revisions to the Risk Analysis, HHS shall provide PBC with a written explanation of the basis of its revisions, including comments and recommendations that PBC can use to prepare a revised Risk Analysis.

4. Upon receiving HHS's notice of required revisions, if any, PBC shall have sixty days to revise the Risk Analysis accordingly and forward to HHS for review and approval. This process shall continue until HHS approves the Risk Analysis.

5. PBC shall review the Risk Analysis annually (or more frequently, if appropriate) and shall promptly update the Risk Analysis in response to environmental or operational changes affecting the security of ePHI. Following an update to the Risk Analysis, PBC shall assess whether its existing security measures are sufficient to protect its ePHI and revise its Risk Management Plan, Policies and Procedures, and training materials and implement additional security measures, as needed.

B. Develop and Implement Risk Management Plan

1. PBC shall develop an enterprise-wide Risk Management Plan to address and mitigate any security risks and vulnerabilities found in the Risk Analysis. The Risk Management Plan shall include a process and timeline for PBC's implementation, evaluation, and revision of its risk remediation activities.

2. Within sixty days of HHS's final approval of the Risk Analysis, PBC shall submit a Risk Management Plan to HHS for HHS's review and approval. PBC may submit a Risk Management Plan developed in response to a Risk Analysis currently underway or previously completed for consideration by HHS for compliance with this provision. [HHS will then review and iterate with PBC accordingly.]

C. Policies and Procedures

1. PBC shall review, and as necessary, develop, maintain, and revise, the written Privacy and Security Policies and Procedures ("policies and procedures") addressing the Minimum Content set forth [above] to confirm compliance with the Federal standards that govern the security of individually identifiable health information.

2. PBC shall provide the policies and procedures identified to HHS for review within 150 days of the Effective Date.

3. Within sixty days of its receipt of PBC's submitted policies and procedures, HHS will inform PBC whether it has any feedback on the submitted policies and procedures.

4. Upon receiving any recommended changes to such policies and procedures from HHS to confirm compliance with the Security Rule, PBC shall have forty-five days to revise such policies and procedures and provide the revised policies and procedures to HHS for review. This process shall continue until HHS confirms that such policies and procedures comply with the requirements of the Security Rule.

5. Within thirty days after receiving HHS' final approval of any revisions to the policies and procedures, PBC shall implement the policies and procedures.

Notes

1. In addition to the immediate compliance demands, which are considerable, PBC was subject to a two-year monitoring program. Do you think this compliance cost is fair? Think about the lawyers, administrators, and staffers involved. It is hard to put a price on this sort of investigation, but it is certainly not cheap. It could easily be larger than the fine.
2. Why is HHS particularly interested in this case? Likely because of the size of the breach (millions) and its preventable nature (a phishing campaign that installed malware). HHS is not doing this because a single person failed. They are doing this because the failure of a single person, or even a small group of people, should not have this kind of consequence. The system should be robust enough to handle such a common mode of attack.

Athens Orthopedic Clinic Resolution Agreement (2020)[164]

On June 26, 2016, a journalist from "www.databreaches.net" notified Athens Orthopedic Clinic (AOC) that "a database of patient records" suspected to belong to AOC was posted online for sale. On June 28, 2016, a hacker group known as "The Dark Overlord" contacted AOC by email and demanded money in return for a complete copy of the database it stole without sale or further disclosure. It was determined, through computer forensic analysis, that the Dark Overlord had obtained a vendor's credentials to AOC's system and used them to gain access on June 14, 2016. While AOC terminated the compromised credentials on June 27, 2016, the Dark Overlord's continued intrusion was not effectively blocked until July 16, 2016.

It was determined that 208,557 individuals were affected by this breach. Due to the breadth of system applications affected, a variety of protected health information (PHI) was exposed including patient demographic information (name, date of birth, social security number, etc.), clinical information (reason for visit, "social history," medications, test results, medical procedures, etc.), and financial/billing information (health insurance information, payment history).

OCR's investigation indicated potential violations of the following provisions of the HIPAA Rules ("Covered Conduct"):

A. The requirement to prevent unauthorized access to the ePHI of 208,557 individuals whose information was maintained in AOC's information systems.

B. Until August 2016, the requirement to maintain copies of AOC's HIPAA policies and procedures.

C. From September 30, 2015 to December 15, 2016, the requirement to implement sufficient hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

[164] The full agreement is available at: https://www.hhs.gov/sites/default/files/athens-orthopedic-ra-cap.pdf

D. Until August 7, 2017, the requirement to enter into business associate agreements with three of its business associates, Quest Records LLC, Total Technology Solutions, and SRS Software LLC.

E. Until January 15, 2018, the requirement to provide its entire workforce with HIPAA training.

F. The requirement to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by AOC.

G. The requirement to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Terms and Conditions

1. **Payment.** AOC agrees to pay to HHS the amount of $1,500,000 ("Resolution Amount"). AOC agrees to pay the Resolution Amount on or before August 7, 2020 by automated clearing house transaction pursuant to written instructions to be provided by HHS.

2. **Corrective Action Plan.** AOC has entered into and agrees to comply with the Corrective Action Plan.

[The terms of the plan regarding Risk Assessment and Management are similar to those of Premera, but the AOC plan includes the following notable additions:]

A. Business Associate Agreements

1. Within 60 days of the Effective Date and annually following the Effective Date, AOC shall review all relationships with vendors and third party service providers to identify business associates. AOC shall provide HHS with the following:

   a. An accounting of AOC's business associates, to include the names of business associates, a description of services provided, the date services began, and a description of the business associate's handling of/interaction with AOC's PHI; and

   b. Copies of the business associate agreements that AOC maintains with each business associate. [AUTH: In an omitted section of Part C, AOC is required to designate a person to ensure that future business associate agreements are properly executed.]

C. Policies and Procedures

AOC shall review and revise its written policies and procedures to comply with the Privacy, Security, and Breach Notification Rules. AOC's policies and procedures shall include, but not be limited to, the minimum content set forth . . . below. Additionally, in light of OCR's investigation, particular revision is required to AOC's policies and procedures relating to:

- Technical access controls for any and all network/server equipment and systems to prevent impermissible access and disclosure of ePHI,
- Technical access control and restriction for all software applications that contain ePHI to ensure authorized access is limited to the minimum amount necessary,
- Technical mechanisms to create access and activity logs as well as administrative procedures to routinely review logs for suspicious events and respond appropriately,
- Termination of user accounts when necessary and appropriate,
- Appropriate configuration of user accounts to comply with the Minimum Necessary Rule,

- Required and routine password changes,
- Password strength and safeguarding,
- Addressing and documenting security incidents,
- Conducting routine, accurate, and thorough risk analyses and implementing corresponding security measures to sufficiently reduce identified risks and vulnerabilities to a reasonable and appropriate level,
- Workforce training,
- Documentation of workforce training,
- Identification of business associates,
- Engaging in compliant business associate agreements,
- Breach notification content requirements.

Notes

1. Again, the term of the corrective action plan is two years. In this case, the plan goes on for several pages beyond that of Premera but offers very similar guidance.
2. Which of the failures outlined by HHS are serious, in your view? Which are preventable? How easy is it to *not* be on the receiving end of one of these actions?
3. Consider the number of HIPAA violations alleged in each of these cases. What do you make of that? Presumably these institutions came to HHS attention solely because of the data breaches, and the other failures of process were discovered during those investigations. Is this a sign that there is a lot of HIPAA noncompliance that goes unreported or investigated? How would some of these failures come to light except via a post-hoc investigation?
4. Business associates can also be targeted with financial penalties directly. In 2020, CHSPSC, an IT and health-information management vendor, was fined $2.3 million for its role in a breach that exposed the personal information of six million people. The HHS specifically emphasized CHSPSC's failure to conduct a risk analysis and failures to implement information-system activity review, security-incident procedures, and access controls.

Yakima Valley Memorial Hospital Press Release (2023)[165]

OCR investigated allegations that several security guards from Yakima Valley Memorial Hospital impermissibly accessed the medical records of 419 individuals. To voluntarily resolve this matter, Yakima Valley Memorial Hospital agreed to pay $240,000 and implement a plan to update its policies and procedures to safeguard PHI and train its workforce members to prevent this type of snooping behavior in the future.

"Data breaches caused by current and former workforce members impermissibly accessing patient records are a recurring issue across the healthcare industry. Health care organizations must ensure that workforce members can only access the patient information needed to do their jobs," said OCR Director Melanie Fontes Rainer. "HIPAA covered entities must have robust policies and procedures in place to ensure PHI is protected from identify theft and fraud."

In May 2018, OCR initiated an investigation of Yakima Valley Memorial Hospital following the receipt of a breach notification report, stating that 23 security guards working in the hospital's emergency department used their login credentials to access patient medical records maintained in Yakima Valley Memorial Hospital's electronic medical record system without a job-related purpose. The information accessed included names, dates of birth, medical record numbers, addresses, certain notes related to treatment, and insurance information.

[165] For unclear reasons, the Resolution Agreement itself contained no description of the alleged conduct, hence presenting the press release. The full text is here, as is a link to the resolution agreement. https://www.hhs.gov/about/news/2023/06/15/snooping-medical-records-by-hospital-security-guards-leads-240-000-hipaa-settlement.html

As a result of the settlement agreement, Yakima Valley Memorial Hospital will be monitored for two years by OCR to ensure compliance with the HIPAA Security Rule. Yakima Valley Memorial Hospital has agreed to take the following steps to bring their organization into compliance with the HIPAA Rules:

- Conduct an accurate and thorough risk analysis to determine risks and vulnerabilities to ePHI;
- Develop and implement a risk management plan to address and mitigate identified security risks and vulnerabilities identified in the risk analysis;
- Develop, maintain, and revise, as necessary, its written HIPAA policies and procedures;
- Enhance its existing HIPAA and Security Training Program to provide workforce training on the updated HIPAA policies and procedures;
- Review all relationships with vendors and third-party service providers to identify business associates and obtain business associate agreements with business associates if not already in place.

Notes

1. There does not appear to be any explanation, either in the HHS documentation or the resulting media coverage, about why the security guards accessed patient information. One could imagine many reasons, ranging from idle curiosity, to intended identity theft, to a misplaced desire to enhance hospital security. A similar enforcement action against University of California at Los Angeles Health System in 2011 was related to hospital staff inappropriately viewing celebrity health data.[166] That action resulted in a $865,000 fine.
2. Note that even here, where we do not have an obvious criminal motive on the part of those who obtained the information, we do not need to show individual damages. There is no allegation that any person suffered financial loss or even emotional harm; it is enough that the data was exposed.
3. In 2023, a highly unusual case involving Manasa Health Center resulted in a fine of $30,000.[167] There, OCR opened an investigation in response to a complaint by a patient alleging that Manasa Health Center posted a response to the patient's negative online review that included specific information regarding the individual's diagnosis and treatment of their mental health condition. OCR's investigation found that Manasa Health Center impermissibly disclosed the PHI of the complaining patient and three other patients in response to their negative online reviews.[168]
4. In 2020, there was a similarly small fine against the City of New Haven for its failure to terminate the access of a former employee. OCR's investigation revealed that on July 27, 2016, eight days after being terminated, a former employee returned to the health department, logged into her old computer with her still active username and password, and downloaded PHI that included patient names, addresses, dates of birth, race/ethnicity, gender, and sexually transmitted disease test results onto a USB drive.[169] Additionally, OCR found that the former employee had shared her username and password with an intern, who continued to use these login credentials to access PHI on New Haven's network after the employee was terminated. OCR's investigation determined that New Haven failed

---

[166] Charles Ornstein, *UCLA Health System Pays $865,000 to Settle Celebrity Privacy Allegations*, PROPUBLICA (July 7, 2011), https://www.propublica.org/article/ucla-health-system-pays-865000-to-settle-celebrity-privacy-allegations.

[167] The resolution agreement is available at https://www.hhs.gov/about/news/2023/06/05/hhs-office-civil-rights-reaches-agreement-health-care-provider-new-jersey-disclosed-phi-response-negative-online-reviews.html

[168] It is unclear to the author what comments were actually made. If anyone can determine what Manasa wrote, please email me.

[169] The resolution agreement is available at https://www.hhs.gov/sites/default/files/new-haven-resolution-agreement-corrective-action-plan.pdf

to conduct an enterprise-wide risk analysis and failed to implement termination procedures, access controls such as unique user identification, and HIPAA Privacy Rule policies and procedures. There was a monetary fine against the city in the amount of $202,400 and, again, a two-year corrective action plan.

This second set of enforcement actions concerns employee misconduct. But the issue here is not so much the poor behavior of the employees as the organization's failure to monitor and limit the access of the employees. Imagine an on-the-ball IT department. It would have detected that a group of employees with no reason to access patient data was doing so (Yakima Valley) and terminated the credentials of the former employee (New Haven). And a well-run office would have made clear that patient data should never be casually disclosed, especially on so public a platform as Google's review page (Manasa). The focus of enforcement in each of these cases is on systemic failure of process.

Consider a more basic HIPAA violation. Imagine you go to a new doctor and are signing your onboarding paperwork. As part of that paperwork, you are asked to sign to indicate that you have received the office's HIPAA form and privacy policy. But, in fact, you have not been given or shown that form.[170] What should happen to that office? Though one could imagine portraying this as a "systematic failure of process," it is more likely the case of a tired, overworked, or lazy employee failing to correctly sort documents. At worst, it is a case of a manager not prioritizing HIPAA paperwork. This sounds like exactly the kind of problem that can be productively addressed by further training of the employee rather than a monetary fine.

4) HIPAA Criminal Enforcement

Under HIPAA, the government may prosecute any "person" who knowingly and in violation of HIPAA:

1. Uses or causes to be used a unique health identifier;
2. Obtains PHI on an individual; or
3. Discloses PHI to another person.

It was initially debated whether this meant the DOJ could prosecute any individual under HIPAA's criminal provisions, whether or not the individual is actually a covered entity. In a 2005 legal opinion, DOJ's Office of Legal Counsel (OLC) stated that only covered entities could be criminally prosecuted under HIPAA, although non-covered individuals could be prosecuted for conspiracy or "aiding and abetting" a covered entity. However, the HITECH Act specifically overturned this interpretation. "A person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization." It is also possible to hold an organization criminally responsible under the principles of corporate criminal liability.

U.S. v. Huping Zhou, 678 F.3d 1110 (2012)

M. SMITH, Circuit Judge:

Defendant–Appellant Huping Zhou, a former research assistant at the University of California at Los Angeles Health System (UHS), accessed patient records without authorization after his employment was terminated. In an information, the government charged him with violating the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which

[170] This has happened several times to the author. In one case, he asked for the HIPAA form and it took staff several minutes to find it. Apparently the form had recently been updated and was not readily available.

imposes a misdemeanor penalty on "[a] person who knowingly *and* in violation of this part . . . obtains individually identifiable health information relating to an individual." 42 U.S.C. § 1320d–6(a)(2) (emphasis added). Zhou moved to dismiss the information because it did not allege that Zhou knew that the statute prohibited him from obtaining the health information. The district court denied the motion to dismiss. Zhou entered a conditional guilty plea, reserving the right to appeal the denial of his motion to dismiss.

Zhou was hired as a research assistant in rheumatology at UHS on February 2, 2003. On October 29, 2003, UHS issued Zhou a notice of intent to dismiss due to "continued serious job deficiencies and poor judgment." On November 12, 2003, after a formal internal grievance hearing, Zhou received a dismissal letter effective November 14, 2003.

After his termination on November 14, 2003, there were at least four instances, on November 17 and 19, in which Zhou accessed patient records without authorization. The information charged Zhou with crimes only for accessing patients' medical information after he was terminated and no longer treating patients at the hospital.

HIPAA provides that: "[a] person who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b)." 42 U.S.C. § 1320d–6(a).

On January 8, 2010, Zhou entered a conditional guilty plea, reserving his right to appeal the court's denial of his motion to dismiss the information. Zhou was sentenced to four months in prison, followed by a year of supervised release, a $2,000 fine, and a $100 special assessment. Zhou filed a timely notice of appeal.

Zhou . . . argues that "knowingly," as used in 42 U.S.C. § 1320d–6(a), modifies "in violation of this part." Under Zhou's interpretation of the statute, a defendant is guilty only if he knew that obtaining the personal healthcare information was illegal.

We reject Zhou's argument because it contradicts the plain language of HIPAA. The statute's misdemeanor criminal penalty applies to an individual who "knowingly *and* in violation of this part . . . obtains individually identifiable health information relating to an individual." 42 U.S.C. § 1320d–6(a)(2) (emphasis added). The word "and" unambiguously indicates that there are two elements of a Section 1320d–6(a)(2) violation: 1) knowingly obtaining individually identifiable health information relating to an individual; and 2) obtaining that information in violation of Title 42 United States Code Chapter 7, Subchapter XI, Part C. Thus, the term "knowingly" applies only to the act of obtaining the health information.

If the statute did not contain "and," then Zhou's argument might be more persuasive. However, we cannot ignore "and" because its presence often dramatically alters the meaning of a phrase. Without "and," the Second Amendment would guarantee "the right of the people to keep bear arms," Leo Tolstoy would have published "War Peace," and James Taylor would have confusingly crooned about "Fire Rain." To overlook "and" would be to violate "an important rule of statutory construction—that every word and clause in a statute be given effect." *United States v. Williams* (9th Cir. 2011).

When the plain language of a statute is clear, it is unnecessary to consider legislative history. If we were to consider it, the legislative history would make no difference.

HIPAA's legislative history indicates that Congress intended broadly to apply this misdemeanor criminal penalty. The House Ways and Means Committee report on this section states that "[p]rotecting the privacy of individuals is paramount" and that "[t]his section reflects the Committee's concern that an individual's privacy be protected." Nothing in the Committee

Report suggests that Congress intended to confine this criminal penalty to those who knew that their actions were illegal.

Moreover, our conclusion is supported by Congress's decision not to require willfulness as an element of the crime. Section 1320d–6(a)(2) uses only the term "knowingly," but other criminal statutes require the crime be committed both "knowingly" and "willfully." In *Bryan v. United States* (1998), the Supreme Court distinguished "knowingly" and "willfully," concluding that "the knowledge requisite to knowing violation of a statute is factual knowledge as distinguished from knowledge of the law." Accordingly, had Congress intended to require a higher level of intent, it would have included "willfully" in Section 1320d–6(a)(2).

Similarly, Section 1320d–6's title indicates a broad scope. The section is titled "Wrongful disclosure of individually identifiable health information." 42 U.S.C. § 1320d–6. Had Congress intended to confine this penalty to people who knew that the disclosure was illegal, the title likely would have limited the scope to knowingly illegal conduct.

Zhou primarily relies on three cases in which the Supreme Court held that other criminal statutes apply only to "knowing" actions. In those statutes, "knowingly" is immediately followed by a series of verbs. The statutes in those cases are ambiguous because "it is not at all clear how far down the sentence the word 'knowingly' is intended to travel." *Liparota v. United States* (1985). Those cases are inapposite because the HIPAA provision at issue here clearly limits "knowingly" to the act of obtaining the information. The placement of "and" eliminates any possible ambiguity.

Zhou also cites HIPAA's civil penalties provision in support of his argument. HIPAA provides an exception to civil liability if "it is established that the person did not know (and by exercising reasonable diligence would have not known) that such person violated such provision." 42 U.S.C. § 1320d–5(a)(1)(A). This argument is unavailing because civil sanctions are entirely separate from the criminal HIPAA provision at issue in this case. Indeed, the presence of this exception in another portion of HIPAA demonstrates that Congress explicitly chose to not include such an exception in Section 1320d–6(a)(2).

Finally, Zhou contends that the rule of lenity requires the court to impute a requirement that the defendant knowingly violated the law. The rule of lenity "requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them." *United States v. Santos* (2008). The rule of lenity does not apply here because the statute is unambiguous.

In sum, we hold that 42 U.S.C. § 1320d–6(a)(2) is not limited to defendants who knew that their actions were illegal. Rather, the defendant need only know that he obtained individually identifiable health information relating to an individual.

Notes

1. After *Zhou*, it seems that the only time "knowing" will save a defendant is when they did not know what they had obtained. In one recent case, the government declined to bring charges because the suspect had obtained PHI using an overly ambitious web-scraping program.[171] Based the broad range of other data the suspect had obtained, it was entirely plausible that they had no idea that PHI was in their collection. Presumably whoever had left PHI exposed in such a way that a mere web scraper could find it was in violation of HIPAA themselves, however.
2. Criminal HIPAA prosecutions are rare. Though liability is technically broad enough to capture illegal access for any reason, many cases involve specific wrongful intent. For instance, in several prosecutions PHI was unlawfully obtained or disclosed by those committing identity theft or health-care fraud. On the other hand, many HIPAA civil

[171] This was relayed by a DOJ employee. Because no charges were brought, no official record is public.

enforcement actions based on employee misconduct could, in theory, have been criminal prosecutions, but it appears to be a deliberate policy choice to not treat them as such.

3. When should a HIPAA violation be criminal? What is the point of adding criminal liability here?

C. Privacy in genetic information

Human genetic information is broadly used for two purposes. The first is identification. Is the genetic information in this sample—a pool of blood, a strand of hair, a glob of saliva—the same as the genetic information in this other sample? The second is prediction. What is the likely health future of the person from whom this sample was collected?

1) Use of genetic information for identification

Though the prediction arena for genetics is both varied and complex, the identification realm tends to be far more straightforward. In terms of litigated cases, identification of genetic samples is primarily a criminal procedure issue. Who left behind the following sample?

Maryland v. King, 569 U.S. 435 (2013)

Justice KENNEDY delivered the opinion of the Court.

In 2003 a man concealing his face and armed with a gun broke into a woman's home in Salisbury, Maryland. He raped her. The police were unable to identify or apprehend the assailant based on any detailed description or other evidence they then had, but they did obtain from the victim a sample of the perpetrator's DNA.

In 2009 Alonzo King was arrested in Wicomico County, Maryland, and charged with first- and second-degree assault for menacing a group of people with a shotgun. As part of a routine booking procedure for serious offenses, his DNA sample was taken by applying a cotton swab or filter paper—known as a buccal swab—to the inside of his cheeks. The DNA was found to match the DNA taken from the Salisbury rape victim. King was tried and convicted for the rape. Additional DNA samples were taken from him and used in the rape trial, but there seems to be no doubt that it was the DNA from the cheek sample taken at the time he was booked in 2009 that led to his first having been linked to the rape and charged with its commission.

The Court of Appeals of Maryland, on review of King's rape conviction, ruled that the DNA taken when King was booked for the 2009 charge was an unlawful seizure because obtaining and using the cheek swab was an unreasonable search of the person. It set the rape conviction aside. This Court granted certiorari and now reverses the judgment of the Maryland court.

I

When King was arrested on April 10, 2009, for menacing a group of people with a shotgun and charged in state court with both first- and second-degree assault, he was processed for detention in custody at the Wicomico County Central Booking facility. Booking personnel used a cheek swab to take the DNA sample from him pursuant to provisions of the Maryland DNA Collection Act (or Act).

On July 13, 2009, King's DNA record was uploaded to the Maryland DNA database, and three weeks later, on August 4, 2009, his DNA profile was matched to the DNA sample collected in the unsolved 2003 rape case.

II

The advent of DNA technology is one of the most significant scientific advancements of our era. The full potential for use of genetic markers in medicine and science is still being explored, but the utility of DNA identification in the criminal justice system is already undisputed. Since the first use of forensic DNA analysis to catch a rapist and murderer in England in 1986, law enforcement, the defense bar, and the courts have acknowledged DNA testing's "unparalleled ability both to exonerate the wrongly convicted and to identify the guilty. It has the potential to significantly improve both the criminal justice system and police investigative practices."

A

The current standard for forensic DNA testing relies on an analysis of the chromosomes located within the nucleus of all human cells. "The DNA material in chromosomes is composed of 'coding' and 'noncoding' regions. The coding regions are known as *genes* and contain the information necessary for a cell to make proteins . . . . Non-protein-coding regions . . . are not related directly to making proteins, [and] have been referred to as 'junk' DNA." The adjective "junk" may mislead the layperson, for in fact this is the DNA region used with near certainty to identify a person. The term apparently is intended to indicate that this particular noncoding region, while useful and even dispositive for purposes like identity, does not show more far-reaching and complex characteristics like genetic traits.

Many of the patterns found in DNA are shared among all people, so forensic analysis focuses on "repeated DNA sequences scattered throughout the human genome," known as "short tandem repeats" (STRs). The alternative possibilities for the size and frequency of these STRs at any given point along a strand of DNA are known as "alleles," and multiple alleles are analyzed in order to ensure that a DNA profile matches only one individual.

The Act authorizes Maryland law enforcement authorities to collect DNA samples from "an individual who is charged with . . . a crime of violence or an attempt to commit a crime of violence; or . . . burglary or an attempt to commit burglary." Maryland law defines a crime of violence to include murder, rape, first-degree assault, kidnapping, arson, sexual assault, and a variety of other serious crimes. Once taken, a DNA sample may not be processed or placed in a database before the individual is arraigned (unless the individual consents). It is at this point that a judicial officer ensures that there is probable cause to detain the arrestee on a qualifying serious offense. If "all qualifying criminal charges are determined to be unsupported by probable cause . . . the DNA sample shall be immediately destroyed." DNA samples are also destroyed if "a criminal action begun against the individual . . . does not result in a conviction," "the conviction is finally reversed or vacated and no new trial is permitted," or "the individual is granted an unconditional pardon."

The Act also limits the information added to a DNA database and how it may be used. Specifically, "[o]nly DNA records that directly relate to the identification of individuals shall be collected and stored." No purpose other than identification is permissible: "A person may not willfully test a DNA sample for information that does not relate to the identification of individuals as specified in this subtitle." Tests for familial matches are also prohibited. The officers involved in taking and analyzing respondent's DNA sample complied with the Act in all respects.

Respondent's DNA was collected in this case using a common procedure known as a "buccal swab." "Buccal cell collection involves wiping a small piece of filter paper or a cotton swab similar to a Q-tip against the inside cheek of an individual's mouth to collect some skin cells." The procedure is quick and painless. The swab touches inside an arrestee's mouth, but it requires no "surgical intrusio[n] beneath the skin," and it poses no "threa[t] to the health or safety" of arrestees.

B

Respondent's identification as the rapist resulted in part through the operation of a national project to standardize collection and storage of DNA profiles. Authorized by Congress and supervised by the Federal Bureau of Investigation, the Combined DNA Index System (CODIS) connects DNA laboratories at the local, state, and national level. Since its authorization in 1994, the CODIS system has grown to include all 50 States and a number of federal agencies. CODIS collects DNA profiles provided by local laboratories taken from arrestees, convicted offenders, and forensic evidence found at crime scenes. To participate in CODIS, a local laboratory must sign a memorandum of understanding agreeing to adhere to quality standards and submit to audits to evaluate compliance with the federal standards for scientifically rigorous DNA testing.

One of the most significant aspects of CODIS is the standardization of the points of comparison in DNA analysis. The CODIS database is based on 13 loci at which the STR alleles are noted and compared. These loci make possible extreme accuracy in matching individual samples, with a "random match probability of approximately 1 in 100 trillion (assuming unrelated individuals)." The CODIS loci are from the non-protein coding junk regions of DNA, and "are not known to have any association with a genetic disease or any other genetic predisposition. Thus, the information in the database is only useful for human identity testing." STR information is recorded only as a "string of numbers"; and the DNA identification is accompanied only by information denoting the laboratory and the analyst responsible for the submission. In short, CODIS sets uniform national standards for DNA matching and then facilitates connections between local law enforcement agencies who can share more specific information about matched STR profiles.

All 50 States require the collection of DNA from felony convicts, and respondent does not dispute the validity of that practice. Twenty-eight States and the Federal Government have adopted laws similar to the Maryland Act authorizing the collection of DNA from some or all arrestees. Although those statutes vary in their particulars, such as what charges require a DNA sample, their similarity means that this case implicates more than the specific Maryland law. At issue is a standard, expanding technology already in widespread use throughout the Nation.

III

A

Although the DNA swab procedure used here presents a question the Court has not yet addressed, the framework for deciding the issue is well established. The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." It can be agreed that using a buccal swab on the inner tissues of a person's cheek in order to obtain DNA samples is a search. Virtually any "intrusio[n] into the human body," will work an invasion of "'cherished personal security' that is subject to constitutional scrutiny." The Court has applied the Fourth Amendment to police efforts to draw blood, scraping an arrestee's fingernails to obtain trace evidence, and even to "a breathalyzer test, which generally requires the production of alveolar or 'deep lung' breath for chemical analysis."

B

To say that the Fourth Amendment applies here is the beginning point, not the end of the analysis. "[T]he Fourth Amendment's proper function is to constrain, not against all intrusions as such, but against intrusions which are not justified in the circumstances, or which are made in an improper manner." "As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Vernonia Sch. Dist. 47J v. Acton* (1995).

In some circumstances, such as "[w]hen faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable."

The instant case can be addressed with this background. The Maryland DNA Collection Act provides that, in order to obtain a DNA sample, all arrestees charged with serious crimes must furnish the sample on a buccal swab. The arrestee is already in valid police custody for a serious offense supported by probable cause. An assessment of reasonableness to determine the lawfulness of requiring this class of arrestees to provide a DNA sample is central to the instant case.

IV

The legitimate government interest served by the Maryland DNA Collection Act is one that is well established: the need for law enforcement officers in a safe and accurate way to process and identify the persons and possessions they must take into custody.

The "routine administrative procedure[s] at a police station house incident to booking and jailing the suspect" derive from different origins and have different constitutional justifications than, say, the search of a place.

First, "[i]n every criminal case, it is known and must be known who has been arrested and who is being tried." *Hiibel v. Sixth Jud. Dist. Ct. of Nev.* (2004). An individual's identity is more than just his name or Social Security number, and the government's interest in identification goes beyond ensuring that the proper name is typed on the indictment. An "arrestee may be carrying a false ID or lie about his identity," and "criminal history records . . . can be inaccurate or incomplete."

A suspect's criminal history is a critical part of his identity that officers should know when processing him for detention. It is a common occurrence that "[p]eople detained for minor offenses can turn out to be the most devious and dangerous criminals." Police already seek this crucial identifying information. They use routine and accepted means as varied as comparing the suspect's booking photograph to sketch artists' depictions of persons of interest, showing his mugshot to potential witnesses, and of course making a computerized **c**omparison of the arrestee's fingerprints against electronic databases of known criminals and unsolved crimes. In this respect the only difference between DNA analysis and the accepted use of fingerprint databases is the unparalleled accuracy DNA provides.

The task of identification necessarily entails searching public and police records based on the identifying information provided by the arrestee to see what is already known about him. The DNA collected from arrestees is an irrefutable identification of the person from whom it was taken. Like a fingerprint, the 13 CODIS loci are not themselves evidence of any particular crime, in the way that a drug test can by itself be evidence of illegal narcotics use. A DNA profile is useful to the police because it gives them a form of identification to search the records already in their valid possession. In this respect the use of DNA for identification is no different than matching an arrestee's face to a wanted poster of a previously unidentified suspect; or matching tattoos to known gang symbols to reveal a criminal affiliation; or matching the arrestee's fingerprints to those recovered from a crime scene.

Second, law enforcement officers bear a responsibility for ensuring that the custody of an arrestee does not create inordinate "risks for facility staff, for the existing detainee population, and for a new detainee." DNA identification can provide untainted information to those charged with detaining suspects and detaining the property of any felon. For these purposes officers must know the type of person whom they are detaining, and DNA allows them to make critical choices about how to proceed.

Third, looking forward to future stages of criminal prosecution, "the Government has a substantial interest in ensuring that persons accused of crimes are available for trials." *Bell v. Wolfish* (1979). A person who is arrested for one offense but knows that he has yet to answer for some past crime may be more inclined to flee the instant charges, lest continued contact with the criminal justice system expose one or more other serious offenses.

Fourth, an arrestee's past conduct is essential to an assessment of the danger he poses to the public, and this will inform a court's determination whether the individual should be released on bail.

This interest is not speculative. In considering laws to require collecting DNA from arrestees, government agencies around the Nation found evidence of numerous cases in which felony arrestees would have been identified as violent through DNA identification matching them to previous crimes but who later committed additional crimes because such identification was not used to detain them.

Present capabilities make it possible to complete a DNA identification that provides information essential to determining whether a detained suspect can be released pending trial. *See, e.g.*, States Brief ("DNA identification database samples have been processed in as few as two days in California, although around 30 days has been average").

Finally, in the interests of justice, the identification of an arrestee as the perpetrator of some heinous crime may have the salutary effect of freeing a person wrongfully imprisoned for the same offense. "[P]rompt [DNA] testing . . . would speed up apprehension of criminals before they commit additional crimes, and prevent the grotesque detention of . . . innocent people." J. DWYER, P. NEUFELD & B. SCHECK, ACTUAL INNOCENCE (2000).

DNA identification is an advanced technique superior to fingerprinting in many ways, so much so that to insist on fingerprints as the norm would make little sense to either the forensic expert or a layperson. The additional intrusion upon the arrestee's privacy beyond that associated with fingerprinting is not significant, and DNA is a markedly more accurate form of identifying arrestees. A suspect who has changed his facial features to evade photographic identification or even one who has undertaken the more arduous task of altering his fingerprints cannot escape the revealing power of his DNA.

The respondent's primary objection to this analogy is that DNA identification is not as fast as fingerprinting, and so it should not be considered to be the 21st-century equivalent. But rapid analysis of fingerprints is itself of recent vintage. The FBI's vaunted Integrated Automated Fingerprint Identification System (IAFIS) was only "launched on July 28, 1999. Prior to this time, the processing of . . . fingerprint submissions was largely a manual, labor-intensive process, taking weeks or months to process a single submission." It was not the advent of this technology that rendered fingerprint analysis constitutional in a single moment. The question of how long it takes to process identifying information obtained from a valid search goes only to the efficacy of the search for its purpose of prompt identification, not the constitutionality of the search. Given the importance of DNA in the identification of police records pertaining to arrestees and the need to refine and confirm that identity for its important bearing on the decision to continue release on bail or to impose of new conditions, DNA serves an essential purpose despite the existence of delays such as the one that occurred in this case.

In sum, there can be little reason to question "the legitimate interest of the government in knowing for an absolute certainty the identity of the person arrested, in knowing whether he is wanted elsewhere, and in ensuring his identification in the event he flees prosecution." W. LAFAVE, SEARCH AND SEIZURE (5th ed. 2012). To that end, courts have confirmed that the Fourth Amendment allows police to take certain routine "administrative steps incident to arrest—*i.e.*, . . . book[ing], photograph[ing], and fingerprint[ing]." *County of Riverside v. McLaughlin* (1991). DNA identification of arrestees, of the type approved by the Maryland statute here at issue, is "no more than an extension of methods of identification long used in

dealing with persons under arrest." In the balance of reasonableness required by the Fourth Amendment, therefore, the Court must give great weight both to the significant government interest at stake in the identification of arrestees and to the unmatched potential of DNA identification to serve that interest.

V

A

By comparison to this substantial government interest and the unique effectiveness of DNA identification, the intrusion of a cheek swab to obtain a DNA sample is a minimal one. True, a significant government interest does not alone suffice to justify a search. The government interest must outweigh the degree to which the search invades an individual's legitimate expectations of privacy.

B

In addition the processing of respondent's DNA sample's 13 CODIS loci did not intrude on respondent's privacy in a way that would make his DNA identification unconstitutional.

First, as already noted, the CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee. While science can always progress further, and those progressions may have Fourth Amendment consequences, alleles at the CODIS loci "are not at present revealing information beyond identification." Katsanis & Wagner, *Characterization of the Standard and Recommended CODIS Markers*, 58 J. FORENSIC SCI. S169 (2013). The argument that the testing at issue in this case reveals any private medical information at all is open to dispute.

And even if non-coding alleles could provide some information, they are not in fact tested for that end. It is undisputed that law enforcement officers analyze DNA for the sole purpose of generating a unique identifying number against which future samples may be matched.

Finally, the Act provides statutory protections that guard against further invasion of privacy. As noted above, the Act requires that "[o]nly DNA records that directly relate to the identification of individuals shall be collected and stored." No purpose other than identification is permissible: "A person may not willfully test a DNA sample for information that does not relate to the identification of individuals as specified in this subtitle."

In light of the context of a valid arrest supported by probable cause respondent's expectations of privacy were not offended by the minor intrusion of a brief swab of his cheeks. By contrast, that same context of arrest gives rise to significant state interests in identifying respondent not only so that the proper name can be attached to his charges but also so that the criminal justice system can make informed decisions concerning pretrial custody. Upon these considerations the Court concludes that DNA identification of arrestees is a reasonable search that can be considered part of a routine booking procedure. When officers make an arrest supported by probable cause to hold for a serious offense and they bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment.

Justice SCALIA, with whom Justice GINSBURG, Justice SOTOMAYOR, and Justice KAGAN join, dissenting.

The Fourth Amendment forbids searching a person for evidence of a crime when there is no basis for believing the person is guilty of the crime or is in possession of incriminating evidence. That prohibition is categorical and without exception; it lies at the very heart of the Fourth Amendment. Whenever this Court has allowed a suspicionless search, it has insisted upon a justifying motive apart from the investigation of crime.

It is obvious that no such noninvestigative motive exists in this case. The Court's assertion that DNA is being taken, not to solve crimes, but to *identify* those in the State's custody, taxes the credulity of the credulous. And the Court's comparison of Maryland's DNA searches to other techniques, such as fingerprinting, can seem apt only to those who know no more than today's opinion has chosen to tell them about how those DNA searches actually work.

[W]hile the Court is correct to note that there are instances in which we have permitted searches without individualized suspicion, "[i]n none of these cases . . . did we indicate approval of a [search] whose primary purpose was to detect evidence of ordinary criminal wrongdoing." *Indianapolis v. Edmond* (2000). That limitation is crucial. It is only when a governmental purpose aside from crime-solving is at stake that we engage in the free-form "reasonableness" inquiry that the Court indulges at length today. To put it another way, both the legitimacy of the Court's method and the correctness of its outcome hinge entirely on the truth of a single proposition: that the primary purpose of these DNA searches is something other than simply discovering evidence of criminal wrongdoing. As I detail below, that proposition is wrong.

B

[T]he Court elaborates at length the ways that the search here served the special purpose of "identifying" King. But that seems to me quite wrong—unless what one means by "identifying" someone is "searching for evidence that he has committed crimes unrelated to the crime of his arrest." At points the Court does appear to use "identifying" in that peculiar sense—claiming, for example, that knowing "an arrestee's past conduct is essential to an assessment of the danger he poses." If identifying someone means finding out what unsolved crimes he has committed, then identification is indistinguishable from the ordinary law-enforcement aims that have never been thought to justify a suspicionless search.

The portion of the Court's opinion that explains the identification rationale is strangely silent on the actual workings of the DNA search at issue here. To know those facts is to be instantly disabused of the notion that what happened had anything to do with identifying King.

King was arrested on April 10, 2009, on charges unrelated to the case before us. That same day, April 10, the police searched him and seized the DNA evidence at issue here. What happened next? Reading the Court's opinion, particularly its insistence that the search was necessary to know "who [had] been arrested," one might guess that King's DNA was swiftly processed and his identity thereby confirmed—perhaps against some master database of known DNA profiles, as is done for fingerprints. After all, was not the suspicionless search here crucial to avoid "inordinate risks for facility staff" or to "existing detainee population?" Surely, then—*surely*—the State of Maryland got cracking on those grave risks immediately, by rushing to identify King with his DNA as soon as possible.

Nothing could be further from the truth. Maryland officials did not even begin the process of testing King's DNA that day. Or, actually, the next day. Or the day after that. And that was for a simple reason: Maryland law forbids them to do so. A "DNA sample collected from an individual charged with a crime . . . *may not* be tested or placed in the statewide DNA data base system prior to the first scheduled arraignment date." And King's first appearance in court was not until three days after his arrest. (I suspect, though, that they did not wait three days to ask his name or take his fingerprints.)

This places in a rather different light the Court's solemn declaration that the search here was necessary so that King could be identified at "every stage of the criminal process." It gets worse. King's DNA sample was not received by the Maryland State Police's Forensic Sciences Division until April 23, 2009—two weeks after his arrest. It sat in that office, ripening in a storage area, until the custodians got around to mailing it to a lab for testing on June 25, 2009—two months after it was received, and nearly *three* since King's arrest. After it was mailed, the data from the lab tests were not available for several more weeks, until July 13, 2009, which is when the test results were entered into Maryland's DNA database . . . .

In fact, if anything was "identified" at the moment that the DNA database returned a match, it was not King—his identity was already known. (The docket for the original criminal charges lists his full name, his race, his sex, his height, his weight, his date of birth, and his address.) Rather, what the August 4 match "identified" was *the previously-taken sample from the earlier crime*.

The most regrettable aspect of the suspicionless search that occurred here is that it proved to be quite unnecessary. All parties concede that it would have been entirely permissible, as far as the Fourth Amendment is concerned, for Maryland to take a sample of King's DNA as a consequence of his conviction for second-degree assault. So the ironic result of the Court's error is this: The only arrestees to whom the outcome here will ever make a difference are those who *have been acquitted* of the crime of arrest (so that their DNA could not have been taken upon conviction). In other words, this Act manages to burden uniquely the sole group for whom the Fourth Amendment's protections ought to be most jealously guarded: people who are innocent of the State's accusations.

Notes

1. The focus of the Court here is on the physical intrusion of the search. The collection of genetic information is a search not because of the intrusion of the government having the genetic information but instead because of the physical cheek swab that collects it in the first place. Does that make sense? Should we be thinking in terms of the vast amount of information contained within DNA, or the *de minimis* intrusion used to collect it?
2. Collecting DNA samples tends to be fairly easy in most cases. People are constantly shedding DNA as they move through the world. Under a well-established line of Fourth Amendment cases, there is no privacy interest in abandoned property, such as trash. *California v. Greenwood*, 486 U.S. 35 (1988). So, where the state has not added protection by statute or the state constitution, law enforcement is permitted to go through a person's trash looking for sources of trace DNA evidence. They can collect the glass you leave behind in a restaurant or the cardboard cup you throw out at Starbucks.
3. In dissent, Scalia makes much of the slow pace of the DNA analysis. Rapid DNA testing might lead to some of the benefits that the majority describes, but others are not applicable to matches that come several months later. Is the majority right to talk about how changes in technology should be anticipated here? Is the majority on firmer ground in a *Gattaca*-like world of instant DNA identification?
4. Though CODIS is not designed to facilitate searches for family DNA matches, private genetic databases like Ancestry.com and 23andMe are. Law enforcement has repeatedly used such sites to identify both criminal suspects and human remains. Sometimes that identification is direct—the sample matches a person with a profile—and sometimes the investigator goes through a convoluted process of tracking second cousins and ancestors to find a match. Many of these databases state that they will not voluntarily cooperate with law enforcement, but they also allow any private person to upload a genetic profile and search for matches. This creates an odd practical result because, as Orin Kerr has observed, "on the internet, no one knows you are a cop." Therefore law enforcement has the practical ability to search without legal process.
5. What is bad about DNA identification being used for law-enforcement purposes? The government regularly collects genetic information from newborns to test for a variety of genetic disorders.[172] Would it be good or dystopian if all babies were enrolled in CODIS upon birth? It would certainly lead to fewer unsolved sexual assault cases in future decades.

[172] See, for example, the mandatory program in Illinois: https://dph.illinois.gov/topics-services/life-stages-populations/newborn-screening.html.

2) Use of genetic information for prediction

Reading the above notes, students may think, "But genetic information is special!" It is not the same arbitrary collection of measurements as a fingerprint. That is correct. Genetic analysis carries with it scientific, pseudo-scientific, emotional, and ideological baggage. One cannot understand the concerns expressed in the late twentieth century regarding genetic information without reference to the eugenics movement of the early twentieth century: the belief that we can scientifically sort and classify people based on their heritage, and that the government should take an active role in promoting the continuation of good and the ending of bad genetic lines. Consider the much-reviled case of *Buck v. Bell*, 274 U.S. 200 (1927), where the Supreme Court upheld a Virginia law permitting the involuntary sterilization of those believed to be mentally unfit.[173] Add in the Holocaust and Jim Crow laws and there emerges a clear Western tradition of discriminating against, sterilizing, and killing people based on their actual or assumed bloodlines. Any program aimed at detecting treatable genetic conditions in infants will run up against concerns like "Will this also be used to identify and kill all the Jews?"[174]

In the private sector, however, genetic information has meaningful applications that have little to do with that ideological heritage. Genetic information can reveal whether someone either has or is likely to have particular genetic conditions. These may directly impact both a person's expected lifespan and their expected health during that lifespan. This is very important information if one is going invest time and energy in a person or be responsible for their medical costs. So lovers, employers, and insurers all have a substantial interest in considering genetic data.

There was a wave of scholarship in the 1990s addressing the moral questions raised by hiding information about genetic conditions from various parties. For instance, is it moral to not tell a prospective spouse that you have the gene for Huntington's, a severe degenerative disorder that typically starts in the 30s or 40s? Or that you have a family history of early-onset Alzheimer's? If one thinks that hiding that information from a spouse is not acceptable, what about hiding that information from a long-term employer? Many faculty work at the same school for decades, and hiring decisions are often made based on hazy projections of future productivity. Perhaps genetics will give us some clue to their future work. Or, in a more economically meaningful domain, consider the career of a pro-athlete. A peek into their health future might be worth millions.

A legal answer to these moral debates took the form of the Genetic Information Nondiscrimination Act of 2008 (GINA), which prohibited some types of genetic discrimination. GINA bars the use of genetic information in health insurance and employment. Title I (42 U.S.C. § 1395ss(x)) prohibits group health plans and health-insurance issuers of group health plans from adjusting premiums or contribution amounts on the "basis of genetic information." Moreover, it forbids group health plans and insurers from requiring genetic testing from plan participants. These organizations can request genetic information for research purposes, but

---

[173] Justice Holmes, in what is likely his worst opinion, wrote: "It is better for all the world, if instead of waiting to execute degenerate offspring for crime, or to let them starve for their imbecility, society can prevent those who are manifestly unfit from continuing their kind. The principle that sustains compulsory vaccination is broad enough to cover cutting the Fallopian tubes. *Jacobson* v. *Massachusetts,* 197 U.S. 11 (1905). Three generations of imbeciles are enough."

[174] For example, consider the data breach at 23andMe in 2023 that appears to have targeted particular groups, including Ashkenazi Jews: Edward Helmore, *Genetic Testing Firm 23andMe Admits Hackers Accessed DNA Data of 7M Users*, THE GUARDIAN (Dec. 5, 2023), https://www.theguardian.com/technology/2023/dec/05/23andme-hack-data-breach.

only if the written request indicates that participation is voluntary and will not impact insurance rates or coverage, among other restrictions.

Title II (42 U.S.C. § 2000ff–1) bars employers from using individuals' genetic information when making hiring, firing, job placement, or promotion decisions. Further, it is illegal for an employer to "request, require, or purchase genetic information with respect to an employee or a family member of the employee" unless the employer satisfies one of several narrow exceptions. Most notably, the employer can collect genetic data "where the employer inadvertently requests or requires family medical history of the employee," where the employer offers health or genetic services, where the employee provides voluntary consent, where the information is purchased from public non-medical sources (books, magazines, newspapers, but not court or medical records), and where the employer needs to in order to comply with a variety of government programs.

GINA can be enforced by the Attorney General, the Equal Employment Opportunity Commission, and private individuals.

Notes

1. Note that discrimination in employment and health insurance is forbidden, but not in life insurance. From a business-model perspective, that makes sense. Health insurance and employment are both shorter-term relationships in most cases. Life insurance may run for decades. If a person can conceal a genetic timebomb from their life-insurance provider, they may spend decades paying premiums that are drastically lower than is proper, raising costs on everyone else when they die earlier than expected.
2. Employers sometimes run afoul of GINA by accident. Consider the prohibition on employers requesting, requiring, or purchasing genetic information on current or prospective employees. Dollar General was sued by the Equal Opportunity Commission because its pre-hiring medical screening process included questions about the medical conditions of applicants' parents, grandparents, and children. *Equal Emp. Opportunity Comm'n v. Dolgencorp, LLC*, No. 2:17-CV-01649-MHH, 2022 WL 2959569 (N.D. Ala. July 26, 2022). It appears that Dollar General was primarily concerned with warehouse workers' vision and blood pressure and did not consider family medical history—but the fact that the medical contractor still asked about family medical history was enough to grant summary judgment for the plaintiff. In contrast, a claim brought by City of Chicago employees was dismissed because it alleged only that their employer had collected basic biometric information from them (height, weight, waist circumference, blood pressure, and cholesterol, glucose, and triglyceride levels) as part of a wellness program, not that genetic information had been obtained. *Williams v. City of Chicago*, 616 F. Supp. 3d 808 (N.D. Ill. 2022).
3. The distinction between genetic and nongenetic information is sometimes slippery. GINA defines an individual's genetic information as information about an "individual's genetic tests," "the genetic tests of family members of such individual," and "the manifestation of a disease or disorder in family members of such individual." 29 U.S.C. § 1191b. GINA further defines "genetic tests" as "an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, that detects genotypes, mutations, or chromosomal changes." Expressly excluded from the definition of "genetic test" is any analysis of proteins or metabolites that is directly related to a manifested medical condition. So an employer can inquire about and consider an employee's current health status, even if their current medical conditions are caused by their genetics. But they cannot seek information that would allow them to predict future, unmanifested conditions or seek specifically genetic information about current conditions.
4. In *Jackson v. Regal Beloit Am., Inc.*, No. CV 16-134-DLB-CJS, 2018 WL 3078760 (E.D. Ky. June 21, 2018) an employer risked GINA liability by allowing their doctor to demand access to a patient's past medical records, which included the kind of family history information described above. Even though the doctor's request was prompted by a prior medical

condition—colon cancer—the request for medical history that included family history violated GINA.

5. Why is genetic information special? Three reasons are usually proposed.

   First, it is unchosen. One's genetics are a consequence of one's ancestors, and one generally does not get to choose one's ancestors.

   Second, genetics are immutable. If one has a genetic propensity for something, that propensity can never be changed. The results of that propensity can be—a person can lose weight, undergo anger management training, or adopt a healthy diet—but the propensity remains. There are fairness concerns with allowing discrimination against a person given these first two factors. It seems ill in keeping with the American Dream and the general notion that everyone has a fair shot in life. So genetic discrimination—even when scientific—has many commonalities with racial discrimination.

   The third reason is qualitatively different. Genetic prediction is scientifically uncertain in many cases. Though some genetic predictions are as simple as a single gene leading inexorably to a medical result, many are not. And genetic science is constantly evolving. The early 2000s saw much discussion of Monoamine oxidase A (MAOA), the so-called warrior gene. It was believed that those possessing this gene were prone to violence and criminality, especially if they grew up in disadvantaged circumstances. Yet more modern methods of genetic analysis have called this line of work into serious question. *See, e.g.*, Nita A. Farahany, Roderick T. Kennedy & Brandon L. Garrett, *Genetic Evidence, MAOA, and State v. Yepez*, 50 N.M. L. REV. 469 (2020) (arguing that the entire line of work is unreliable and fatally flawed). Also, genetic propensities for complex behavioral traits (aggression) and personal characteristics (intelligence) are likely to be perpetually hazy. A small effect showing that a certain combination of genes makes someone slightly more aggressive or intelligent may be scientifically valuable, but less useful than, say, watching the person's behavior or giving them a test of academic achievement.

6. More on the prediction side than the identification side is the use of genetic testing to confirm family relationships. This comes up in ancestry testing, paternity cases, and family reunification—think undocumented immigration and refugees. Social media is full of stories of people finding out that their biological fathers were not who they believed, or that they were adopted. There is an entire movement of donor-conceived people whose parents were lied to about the source of the sperm used to create the child.[175]

[175] For one of the sweeter stories, see Evelyn Frick, *This Jewish TikToker Made Us Cry with Her Latke Story*, THE NOSHER (Dec. 13, 2023), https://www.myjewishlearning.com/the-nosher/this-jewish-tiktoker-made-us-cry-with-her-latke-story/. For the less happy side of that story, see https://www.distractify.com/p/is-our-father-a-true-story.

VIII. Financial Privacy

A. The Common Law 393
Dwyer v. American Express Company, 652 N.E.2d 1351 (Ill App. Ct.1995) 393

B. Gramm–Leach–Bliley Act 397

C. Fair Credit Reporting Act 400
1) Scope of the Act 400
2) Protections under the FCRA 401
United States v. Spokeo, Inc., CV12-05001 (C.D. Cal. 2012) 403
Erickson v. First Advantage Background Services Corp., 981 F.3d 1246 (11th Cir. 2020) 406
3) Federal Standing and FCRA claims 410
TransUnion LLC v. Ramirez, 594 U.S. 413 (2021) 412

Under the American sectoral approach to privacy, the amount of privacy you have varies greatly industry by industry. Sometimes a great deal of privacy protection is offered—think of wiretap law and the medical domain. But sometimes much less privacy is provided than the average person might expect. As we will see here, the financial domain gets less protection than does the medical domain and the protections that are offered are more limited in scope.

Also relevant to the protection of financial data are state data breach laws and, where available, comprehensive state privacy laws. These are covered in the Consumer Privacy chapter.

A. The Common Law

All privacy statutes are additive to the common law, so we will begin there. What happens when a consumer challenges the sale of financial information to data brokers under the privacy torts?

Dwyer v. American Express Company, 652 N.E.2d 1351 (Ill App. Ct.1995)

JUSTICE BUCKLEY delivered the opinion of the court:

Plaintiffs, American Express cardholders, appeal the circuit court's dismissal of their claims for invasion of privacy and consumer fraud against defendants for their practice of renting information regarding cardholder spending habits.

On May 13, 1992, the New York Attorney General released a press statement describing an agreement it had entered into with defendants. The following day, newspapers reported defendants' actions which gave rise to this agreement. According to the news articles, defendants categorize and rank their cardholders into six tiers based on spending habits and then rent this information to participating merchants as part of a targeted joint-marketing and sales program. For example, a cardholder may be characterized as “Rodeo Drive Chic” or “Value Oriented.” In order to characterize its cardholders, defendants analyze where they shop and how much they spend, and also consider behavioral characteristics and spending histories. Defendants then offer to create a list of cardholders who would most likely shop in a particular store and rent that list to the merchant.

Defendants also offer to create lists which target cardholders who purchase specific types of items, such as fine jewelry. The merchants using the defendants' service can also target shoppers in categories such as mail-order apparel buyers, home-improvement shoppers,

electronics shoppers, luxury lodgers, card members with children, skiers, frequent business travelers, resort users, Asian/European travelers, luxury European car owners, or recent movers. Finally, defendants offer joint-marketing ventures to merchants who generate substantial sales through the American Express card. Defendants mail special promotions devised by the merchants to its cardholders and share the profits generated by these advertisements.

On May 14, 1992, Patrick E. Dwyer filed a class action against defendants. His complaint alleges that defendants intruded into their cardholders' seclusion, commercially appropriated their cardholders' personal spending habits, and violated the Illinois consumer fraud statute and consumer fraud statutes in other jurisdictions.

Invasion of Privacy

There are four branches of the privacy invasion tort identified by the Restatement (Second) of Torts. These are: (1) an unreasonable intrusion upon the seclusion of another; (2) an appropriation of another's name or likeness; (3) a public disclosure of private facts; and (4) publicity which reasonably places another in a false light before the public.

In *Melvin v. Burling* (1986), the court set out four elements which must be alleged in order to state a cause of action: (1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion which is offensive or objectionable to a reasonable man; (3) the matter upon which the intrusion occurs is private; and (4) the intrusion causes anguish and suffering.

Plaintiffs' allegations fail to satisfy the first element, an unauthorized intrusion or prying into the plaintiffs' seclusion. The alleged wrongful actions involve the defendants' practice of renting lists that they have compiled from information contained in their own records. By using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.

Plaintiffs claim that because defendants rented lists based on this compiled information, this case involves the disclosure of private financial information and most closely resembles cases involving intrusion into private financial dealings, such as bank account transactions.

However, we find that this case more closely resembles the sale of magazine subscription lists, which was at issue in *Shibley v. Time, Inc.* (Ohio Ct. App. 1975). In *Shibley,* the plaintiffs claimed that the defendant's practice of selling and renting magazine subscription lists without the subscribers' prior consent "constitut[ed] an invasion of privacy because it amount[ed] to a sale of individual 'personality profiles,' which subjects the subscribers to solicitations from direct mail advertisers."

The *Shibley* court found that an Ohio statute, which permitted the sale of names and addresses of registrants of motor vehicles, indicated that the defendant's activity was not an invasion of privacy. The *Shibley* court . . . held:

> "The right to privacy does not extend to the mailbox and therefore it is constitutionally permissible to sell subscription lists to direct mail advertisers. It necessarily follows that the practice complained of here does not constitute an invasion of privacy even if appellants' unsupported assertion that this amounts to the sale of 'personality profiles' is taken as true because these profiles are only used to determine what type of advertisement is to be sent."

Defendants rent names and addresses after they create a list of cardholders who have certain shopping tendencies; they are not disclosing financial information about particular cardholders. These lists are being used solely for the purpose of determining what type of advertising should be sent to whom. We also note that the Illinois Vehicle Code authorizes the

Secretary of State to sell lists of names and addresses of licensed drivers and registered motor-vehicle owners. Thus, we hold that the alleged actions here do not constitute an unreasonable intrusion into the seclusion of another. We so hold without expressing a view as to the appellate court conflict regarding the recognition of this cause of action.

Considering plaintiffs' appropriation claim, the elements of the tort are: an appropriation, without consent, of one's name or likeness for another's use or benefit. This branch of the privacy doctrine is designed to protect a person from having his name or image used for commercial purposes without consent. According to the Restatement, the purpose of this tort is to protect the "interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness."

Plaintiffs claim that defendants appropriate information about cardholders' personalities, including their names and perceived lifestyles, without their consent. Defendants argue that their practice does not adversely affect the interest of a cardholder in the "exclusive use of his own identity," using the language of the Restatement. Defendants also argue that the cardholders' names lack value and that the lists that defendants create are valuable because "they identify a useful aggregate of potential customers to whom offers may be sent."

[W]e again follow the reasoning in *Shibley* and find that plaintiffs have not stated a claim for tortious appropriation because they have failed to allege the first element. Undeniably, each cardholder's name is valuable to defendants. The more names included on a list, the more that list will be worth. However, a single, random cardholder's name has little or no intrinsic value to defendants (or a merchant). Rather, an individual name has value only when it is associated with one of defendants' lists. Defendants create value by categorizing and aggregating these names. Furthermore, defendants' practices do not deprive any of the cardholders of any value their individual names may possess.

Consumer Fraud Act

Plaintiffs' complaint also includes a claim under the Illinois Consumer Fraud Act. To establish a deceptive practice claim, a plaintiff must allege and prove (1) the misrepresentation or concealment of a material fact, (2) an intent by defendant that plaintiff rely on the misrepresentation or concealment, and (3) the deception occurred in the course of conduct involving a trade or commerce.

According to the plaintiffs, defendants conducted a survey which showed that 80% of Americans do not think companies should release personal information to other companies. Plaintiffs have alleged that defendants did disclose that it would use information provided in the credit card application, but this disclosure did not inform the cardholders that information about their card usage would be used. It is highly possible that some customers would have refrained from using the American Express Card if they had known that defendants were analyzing their spending habits. Therefore, plaintiffs have sufficiently alleged that the undisclosed practices of defendants are material and deceptive.

As to the second element, the Act only requires defendants' intent that plaintiffs rely on the deceptive practice. Actual reliance is not required. "A party is considered to intend the necessary consequences of his own acts or conduct." *Warren v. LeMay* (Ill. App. Ct. 1986). When considering whether this element is met, good or bad faith is not important and innocent misrepresentations may be actionable. Defendants had a strong incentive to keep their practice a secret because disclosure would have resulted in fewer cardholders using their card. Thus, plaintiffs have sufficiently alleged that defendants intended for plaintiffs to rely on the nondisclosure of their practice.

The third element is not at issue in this case. However, defendants argue that plaintiffs have failed to allege facts that might establish that they suffered any damages. The Illinois Consumer Fraud Act provides a private cause of action for damages to "[a]ny person who suffers

damage as a result of a violation of th[e] Act." Defendants contend, and we agree, that the only damage plaintiffs could have suffered was a surfeit of unwanted mail. We reject plaintiffs' assertion that the damages in this case arise from the disclosure of personal financial matters. Defendants only disclose which of their cardholders might be interested in purchasing items from a particular merchant based on card usage. Defendants' practice does not amount to a disclosure of personal financial matters. Plaintiffs have failed to allege how they were damaged by defendants' practice of selecting cardholders for mailings likely to be of interest to them.

Plaintiffs argue that the consumer fraud statutes of other States allow recovery of mental anguish even if no other damages are pled or proved. Apparently, plaintiffs would like this court to assume that a third party's knowledge of a cardholder's interest in their goods or services causes mental anguish to cardholders. Such an assumption without any supporting allegations would be wholly unfounded in this case. Therefore, we hold that plaintiffs have failed to allege facts that might establish that they have suffered any damages as a result of defendants' practices.

Notes

1. *Dwyer* is a state court case, but it stands in for a generally accepted way of thinking. The data generated from a person's interactions with a company are not private from that company. The company is therefore free to use that data however it likes absent a promise or statute to the contrary. You should see echoes of the third-party doctrine here.
2. As we will see when we reach the Federal Trade Commission's Section 5 authority, the subject of privacy promises has received a great deal of attention over the past thirty years. Here, the court considered a parallel claim under an Illinois statute and rejected it on the grounds that there is no harm in this case. Do you agree? Are the plaintiffs harmed here? Or, rather, could a properly pled complaint make a plausible claim of harm?
3. The court in *Dwyer* is being simplistic, or perhaps out of date, in describing drivers' license information as available for public sale. This is sharply limited under the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (requiring express consent to disclose driver data for use in "bulk distribution for surveys, marketing or solicitations"). Yet courts still make statements such as "matters of public record like a name, address, date of birth, and marriage are not private facts that give rise to a claim." *Bonilla v. Ancestry.com Operations Inc.*, 574 F.Supp.3d 582, 597 (N.D. Ill. 2021). This is contrasted with examples of private facts, such as "family problems, romantic interests, sex lives, health problems, future work plans and criticism of [an employer]." *Vega v. Chicago Park District*, 958 F.Supp.2d 943, 959 (N.D. Ill. 2013).
4. The subject of mailing lists may seem quaint, but it continues to arise. In a case filed in 2021, a plaintiff alleged that Hearst Communications, the magazine distributor responsible for *Good Housekeeping, Esquire, Car and Driver, Men's Health*, and *Cosmopolitan*, among others, was selling subscription list information and that this violated the Illinois Right of Publicity Act (which superseded the common law cause of action used in *Dwyer*). The court disagreed, "while Ms. Huston alleges that Hearst made mailing lists of its subscribers available for others to purchase so that they can send advertisements to the subscribers, this alone does not meet the 'commercial purposes' requirement under the [act]." *Huston v. Hearst Communications, Inc.*, No. 21-CV-1196, 2022 WL 385176 (C.D. Ill. Feb. 7, 2022).
   The act defines commercial purpose as: "the public use or holding out of an individual's identity (i) on or in connection with the offering for sale or sale of a product, merchandise, goods, or services; (ii) for purposes of advertising or promoting products, merchandise, goods, or services; or (iii) for the purpose of fundraising." Courts have interpreted that language to require the use of a person's identity to advertise an unrelated product or service. Here, the use of plaintiff's identity was *as* a product, which is different and unprotected.

B. Gramm–Leach–Bliley Act

In 1999, Congress passed the Gramm–Leach–Bliley Act (GLBA) to allow for greater aggregation in the financial services industry. As it removed barriers to mergers and cooperation between financial institutions, it also created a series of privacy protections.

Scope. GLBA applies to "financial institutions," defined as any institution that is "significantly engaged" in financial activities or significantly engaged in activities incidental to such financial activities. 12 U.S.C. § 1843 defines an activity as "financial in nature or incidental to a financial activity" if it includes, among other things, lending, exchanging, investing, insuring, guaranteeing, indemnifying, providing financial or investment advisory services, underwriting, and acquiring or controlling shares or ownership interests.

The Federal Trade Commission offers two factors in determining whether an institution is "significantly engaged" in financial activities: 1) the existence of a formal arrangement and 2) how often the business engages in a financial activity.[176] Regarding the first factor, the FTC explains that a bartender who "runs a tab" for customers is not considered significantly engaged in financial activities, whereas a retailer that offers credit directly to consumers by issuing its own credit card would be covered. For the second factor, the FTC states that a retailer allowing occasional layaway payments is not significantly engaged in a financial activity. In contrast, a business that regularly wires money to and from consumers is considered significantly engaged in a financial activity. The Code of Federal Regulations provides additional examples of what constitutes a financial institution, including: a retailer issuing its own credit card; a car dealership engaged in leases longer than 90 days; a check-cashing business; an income tax preparer; and a finder that facilitates transactions. See 16 C.F.R. § 314.2.

Nonpublic Personal Information. GLBA protects only nonpublic personal information, defined as a consumer's personally identifiable financial information or any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personally identifiable financial information. Information on the names and addresses of customers of an entity that is not a financial institution or information that does not identify a consumer is not personally identifiable financial information.

Consumers vs. customers. GLBA distinguishes between "consumers" and "customers." A consumer is someone who obtains or has obtained a financial product or service from a financial institution to use primarily for personal, family, or household purposes or for that person's legal representative. Only an individual may be a consumer, and companies or individuals seeking a financial institution's product or service for a business purpose are not consumers.

Customers are a subclass of consumers that have a continuing relationship with a financial institution, such as by having an account there. A former customer who no longer has a continuing relationship with the financial institution is a consumer.

A financial institution must provide customers with a full privacy notice at the beginning of the customer relationship and provide annual updates. This must include information about policies concerning the disclosure of personal information to affiliates and other companies, as well as the categories of information that are disclosed. However, a consumer only receives a privacy notice when the financial institution intends to share the consumer's nonpublic personal information with a nonaffiliated third party for purposes other than processing transactions.

---

[176] Fed. Trade Comm'n, How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act (July 2002), https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.

In 2018, PayPal's Venmo violated GLBA's clear and conspicuous privacy notice requirement by hyperlinking its privacy notice in the Venmo app. Customers were not required to acknowledge receipt of Venmo's privacy policy as a necessary step to obtaining Venmo's services, and the hyperlink was in gray text on a light gray background. The FTC determined that this was a violation of 16 C.F.R. § 313.9, which requires financial institutions to deliver privacy and opt-out notices in a way that a consumer can reasonably expect to receive them.[177]

Notice Content. A privacy notice must contain specific disclosures. However, a financial institution may provide to consumers who are not also customers a "short form" initial notice together with an opt-out notice stating that the institution's full privacy notice is available upon request. The privacy notice must contain: (1) categories of information collected; (2) categories of information disclosed; (3) categories of affiliates and nonaffiliated third parties to whom the institution may disclose information; (4) policies and practices with respect to the treatment of former customers' information; (5) categories of information disclosed to nonaffiliated third parties that perform services for the institution or functions on the institution's behalf and categories of third parties with whom the institution has contracted; (6) an explanation of the opt-out right and methods for opting out; (7) any opt-out notices that the institution must provide under the Fair Credit Reporting Act with respect to affiliate information sharing; (8) policies and practices for protecting the security and confidentiality of information; and (9) a statement that the institution makes disclosures to other nonaffiliated third parties for everyday business purposes or as permitted by law.

Nonaffiliated third party. A "nonaffiliated third party" is any person except a financial institution's affiliate or a person employed jointly by a financial institution and a company that is not the institution's affiliate. An "affiliate" of a financial institution is any company that controls, is controlled by, or is under common control with the financial institution.

Information sharing. Consumers must be given the right to "opt out" of, or prevent, a financial institution from disclosing nonpublic personal information about them to a nonaffiliated third party. Consumers do not have a right to opt out of information sharing with affiliates. Nor can consumers prevent sharing with nonaffiliated third parties that perform services for the financial institution or to function on its behalf, including marketing the institution's own products or services or those offered jointly by the institution and another financial institution. The exception is permitted only if the financial institution provides an initial notice of these arrangements and by contract prohibits the third party from disclosing or using the information beyond the specified purposes. Financial institutions can also make disclosures to protect against actual or potential fraud.

Limitations on Disclosure of Account Numbers. A financial institution must not disclose an account number or similar form of access number or access code for a credit card, deposit, or transaction account to any nonaffiliated third party (other than a consumer reporting agency) for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.

Safeguards Rule and Data Breach. The Safeguards Rule requires financial institutions to "develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information." This information security program must be written and must be appropriate to the size and nature of the business, as well as the sensitivity of handled information. Among other requirements, a financial institution must also have a contract with its service providers allowing it to monitor and assess their own safeguards. In 2023, the FTC amended the Rule to include notice obligations based on the New York Department of Financial Services' 23 NYCRR § 500. Under the amended Safeguards Rule, non-banking financial institutions, such as financial technology

[177] Complaint, *In the Matter of PAYPAL, INC.* (FTC 2018) (available at https://www.ftc.gov/system/files/documents/cases/venmo_complaint.pdf).

companies, mortgage brokers, credit counselors, financial planners, tax preparers, motor vehicle dealers, and payday lenders, must report data breaches involving at least 500 consumers to the FTC.

Breaches are described as the "acquisition of unencrypted customer information without the authorization of the individual to which the information pertains." Customer information is considered unencrypted for this purpose if the encryption key was accessed by an unauthorized person. Unauthorized acquisition is presumed when there has been unauthorized access. To overcome this presumption, the institution must provide reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition.

There are content requirements to the notice as well: (1) the name and contact information of the reporting financial institution; (2) a description of the types of information that were involved in the notification event; (3) if the information is possible to determine, the date or date range of the notification event; (4) the number of consumers affected; (5) a general description of the notification event; (6) whether any law enforcement official has provided the financial institution with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the Federal Trade Commission to contact the law enforcement official. The notice must be filed electronically on the FTC's website. 16 C.F.R. § 314.4(j)(1).

Notice must be provided as soon as possible and no later than thirty days after discovery. The discovery period is triggered by the knowledge of a notification event by anyone within the institution, other than the person committing the breach, such as an employee, officer, or other agent. The FTC will only grant extensions to public notice if law enforcement directly makes such a request.

Enforcement. GLBA is enforced by the FTC and federal banking regulators and does not provide a private right of action. Courts have sometimes been willing to recognize data breaches as a violation of duty of care under negligence per se. Under tort law, negligence per se is found when the defendant has violated a regulation designed to protect the same class of persons as the plaintiff, the same type of harm as the plaintiff, and the particular hazard that led to the plaintiff's harm. For example, a California federal court upheld New York plaintiffs' GLBA claim under New York's negligence per se law in *In re Experian Data Breach Litigation,* No. SACV-151592 AG (DFMx), 2016 WL 7973595, at *4 (C.D. Cal. Dec. 29, 2016). Such negligence per se actions would presumably not allow for private enforcement of any of GLBA's more technical provisions, however.

Notes

1. GLBA has generated a great deal of paperwork for financial institutions. If you go into privacy practice, you will likely need to write and read GLBA-mandated privacy notices. But how much privacy is being protected here? On one hand, GLBA mirrors HIPAA in having covered entities and affiliates, imposing data security and data breach notification requirements, and requesting consent for some information sharing. But the consent requirement here has many more holes. Information can be freely shared with affiliate financial institutions. Nonaffiliate sharing is on an opt-out rather than opt-in basis and has broad exceptions for joint marketing ventures. The typical GLBA enforcement action is more concerned with data security than data privacy.
2. Though current data does not appear to be available, surveys from around the year 2000 suggest that virtually no one (0.5%) opts out under GLBA and a majority of people do not even claim to have read the provided privacy notices. Edward J. Janger & Paul M. Schwartz, *The Gramm–Leach–Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230 (2002).
3. Reconsidering *Dwyer*. The *Dwyer* case predates GLBA, but under its rules little would change. American Express would need to send its users an annual privacy notice stating

that information would be shared with third-party marketers. If those marketers were not affiliates, American Express would need to allow its users to opt out. American Express could bury this opt-out notice at the end of a lengthy privacy policy, however, and it could reasonably expect that almost no one would actually opt out.

4. *In defense of GLBA*. GLBA had the effect of making financial institutions think about privacy, prioritize data security, and at least figure out where they were sending private customer information. This may sound like an extremely modest set of benefits, but consider a world in which financial institutions were *not* thinking about where they sent data. Some financial institutions even limited their data sharing after GLBA. Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law,* 86 MINN. L. REV. 1263 (2002).

C. Fair Credit Reporting Act

Much information-gathering and processing is relatively free from federal regulation. There is nothing to stop a person from using Google or Bing to do research on a potential hire, friend, or romantic partner. The Fair Credit Reporting Act (FCRA) creates a separate ecosystem where the rules are far different, however. Companies regulated under the FCRA need to abide by an extensive list of regulations that are aimed at ensuring the accuracy of the information contained in their files and protecting the privacy of the people described in them.

1) Scope of the Act

The FCRA regulates the behavior of "consumer reporting agencies." The best way to understand the scope of the statute is to examine the relevant definitions:

> The term "consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of *preparing or furnishing consumer reports*. 15 U.S.C. § 1681a(f) (emphasis added).

This naturally leads to the question "what is a consumer report?"

> The term "consumer report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part *for the purpose of serving as a factor in establishing the consumer's eligibility for*
>
> (A) credit or insurance to be used primarily for personal, family, or household purposes;
>
> (B) employment purposes; or
>
> (C) any other purpose authorized under [§ 1681b].

15 U.S.C. § 1681a(d) (emphasis added). This is most easily unpacked from the bottom up. A consumer report is an evaluation of a person's creditworthiness or general character that is created to be used for credit, insurance, or employment purposes. A consumer reporting agency is an organization that regularly prepares such reports and furnishes them to third parties. So, all of this revolves around the purpose limitation: if you make such reports to help other people evaluate targets for credit, insurance, employment (or similar), you are a consumer reporting

agency. If you make them only for other purposes (for example, for entertainment, stalking, or general nosiness), you are not.

2) Protections under the FCRA

There are two main sets of protections offered under the FCRA. First, a consumer report should only be released to a person/entity that the consumer reporting agency believes will use it for a "permissible purpose." Second, a person about whom a report is prepared has a series of rights intended to ensure that the report is accurate and not released needlessly.

Permissible purposes. Consumer reporting agencies may furnish a consumer report: in response to a written request by the consumer, in response to an appropriate subpoena or court order, to a state or local child support enforcement agency, or to an entity it believes:

> (A) intends to use the information in connection with a credit transaction involving the consumer … and involving the extension of credit to, or review or collection of an account of, the consumer; or
>
> (B) intends to use the information for employment purposes; or
>
> (C) intends to use the information in connection with the underwriting of insurance involving the consumer; or
>
> (D) intends to use the information in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status; or
>
> (E) intends to use the information, as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation; or
>
> (F) otherwise has a legitimate business need for the information—
>
> > (i) in connection with a business transaction that is initiated by the consumer; or
> >
> > (ii) to review an account to determine whether the consumer continues to meet the terms of the account.

15 U.S.C. § 1681b(a). This list is long, but relatively limited in scope. In short, consumer reports can be obtained when credit, insurance, or employment are at issue. The broadest permissible purposes are those found in F(i) and F(ii). F(i) notably requires a legitimate business need coupled with *initiation by the consumer*. This means that a company cannot request a report because it is thinking of initiating a transaction with a consumer and is wondering if the consumer would be a good candidate for it. F(ii) involves the evaluation of an ongoing credit account, so there must obviously be such an account. For more about the limits of these exceptions, see *Smith v. Bob Smith Chevrolet, Inc.*, 275 F.Supp.2d 808 (W.D. Ky. 2003).[178]

Further, there are some limitations on when each of these purposes can be invoked. For example, the disclosure of a consumer report for employment purposes requires "clear and conspicuous" disclosure that the report will be obtained and consent from the consumer.[179] 15 U.S.C. § 1681b(b)(2)(A). Also, if an entity wishes to rely on (A) or (C) from the list of permissible purposes to get a consumer report for a transaction *not* initiated by the consumer, the entity

---

[178] I am repeatedly amazed that this is a real case and that the caption is not the creation of either AI or a bored law professor. Feel free to look it up if you doubt me.

[179] Though it initially appears that this disclosure and consent must be in writing, it can be electronic or oral if the individual does not apply in person.

must either obtain consent or the transaction must consist of a firm offer of credit or insurance. Consumers also have the right to opt out of receiving such unsolicited offers of credit.

Consumer reporting agencies are required by statute to police these purpose limitations to some degree. Specifically,

> Every consumer reporting agency shall maintain reasonable procedures designed … to limit the furnishing of consumer reports to the purposes listed under section 1681b of this title. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. Every consumer reporting agency shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user a consumer report. No consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a purpose listed in section 1681b of this title. 15 U.S.C. § 1681e(a).

This is not an ambitious set of verification requirements, but it at least requires some amount of vetting and creates a clear paper trail that can be the subject of a later investigation.

Taken as a whole, the definition of consumer reporting agency and this restriction to permissible purposes work together. If an entity is in the business of assembling reports for covered purposes, it should only assemble reports for those purposes. If an entity is *not* in the business of assembling reports for covered purposes, it should never assemble such reports.

Accuracy, adverse actions, and other protections. In addition to ensuring that reports are only used for permissible purposes, the FCRA also seeks to ensure that the reports are accurate and that consumers are aware of their rights under the statute. § 1681e therefore continues:

> **(b) Accuracy of report.** Whenever a consumer reporting agency prepares a consumer report it shall follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates.
>
> **(c) Disclosure of consumer reports by users allowed.** A consumer reporting agency may not prohibit a user of a consumer report furnished by the agency on a consumer from disclosing the contents of the report to the consumer, if adverse action against the consumer has been taken by the user based in whole or in part on the report.
>
> **(d) Notice to Users and Furnishers of Information**
>
> > **(1) Notice requirement.** A consumer reporting agency shall provide to any person—
> >
> > > (A) who regularly and in the ordinary course of business furnishes information to the agency with respect to any consumer; or
> > >
> > > (B) to whom a consumer report is provided by the agency;
> >
> > a notice of such person's responsibilities under this title.
> >
> > **(2) Content of notice.** The Burea u shall prescribe the content of notices under paragraph (1), and a consumer reporting agency shall be in compliance with this subsection if it provides a notice under paragraph (1) that is substantially similar to the Bureau prescription under this paragraph.

When an entity that has received a consumer report wishes to take an adverse action—a denial of credit, hiring, promotion, etc.—based, at least in part, on it, that entity must tell the person it is doing so and provide the person with contact information for whomever generated the report. A person subject to an adverse action is entitled to a free copy of their consumer report, as is a person who is a victim of identity theft. This means that such a person has a potential remedy: they can examine the report and seek to correct any inaccuracies contained therein.

The accuracy requirement in the FCRA is something of a puzzle, however. "Reasonable procedures" appears to set a low bar, but "maximum possible accuracy" sounds like an extremely high one. As we shall see, courts have generally required consumer reporting agencies to be accurate in reporting what they are told, but not to be proactive in checking or analyzing the information to detect errors.

Some information is also excluded from consumer reports by statute. Specifically, bankruptcies more than ten years old; paid tax liens, accounts in collections, arrest records,[180] and "any other adverse item of information, other than records of convictions of crimes which antedates the report by more than seven years" must be excluded. These exclusions only apply when the credit or insurance at issue is under $150,000 or the employment at issue pays under $75,000 per year. 15 U.S.C. § 1681c.

Enforcement. The FCRA can be enforced both by private lawsuits as well as by agency action. "Any person who willfully fails to comply with any requirement imposed under this title with respect to any consumer is liable to that consumer" for actual damages, statutory damages of up to $1,000, and "in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court." 15 U.S.C. § 1681n(a). Obtaining a consumer report under false pretenses would fall under this provision, and also potentially carries with it a prison term. 15 U.S.C. § 1681q. Negligent violations of the FCRA allow for actual damages and attorney fees, but not punitive or statutory damages. 15 U.S.C. § 1681o.

The FTC can bring civil actions to enforce the FCRA and can pursue damages of up to $2,500 per knowing violation. Various other agencies have some enforcement authority as well, most notably the Consumer Financial Protection Bureau.

United States v. Spokeo, Inc., CV12-05001 (C.D. Cal. 2012)

Complaint for Civil Penalties, Injunction and Other Relief

Spokeo assembles consumer information from "hundreds of online and offline sources," such as social networking sites, data brokers, and other sources to create consumer profiles, which Defendant promotes as "coherent people profiles" and "powerful intelligence." These consumer profiles identify specific individuals and display such information as the individual's physical address, phone number, marital status, age range, or email address. Spokeo profiles are further organized by descriptive headers denoting, among other things, a person's hobbies, ethnicity, religion, or participation on social networking sites, and may contain photos or other information, such as economic health graphics, that Spokeo attributes to a particular individual. Among other things, Spokeo sells the profiles through paid subscriptions, which provide a set number of searches based on subscription level, as well as through Application Program Interfaces ("API") that provide customized and/or higher volume access.

Since at least 2008, Spokeo has provided its consumer profiles to businesses, including entities operating in the human resources ("HR"), background screening, and recruiting

[180] If the statute of limitations for the given offense is longer than seven years, then that period governs instead.

industries, to serve as a factor in deciding whether to interview a job candidate or whether to hire a candidate after a job interview.

a. Spokeo entered into API user agreements with, and provided high volume access to, paying business customers including entities operating in the human resources background screening, and recruiting industries.
b. ln its marketing and advertising, the company has promoted the use of its profiles as a factor in deciding whether to interview a job candidate or whether to hire a candidate after a job interview. Spokeo purchased thousands of online advertising keywords including terms targeting employment background checks, applicant screening, and recruiting. Spokeo ran online advertisements with taglines to attract recruiters and encourage HR professionals to use Spokeo to obtain information about job candidates' online activities.
c. Spokeo has affirmatively targeted companies operating in the human resources, background screening, and recruiting industries. It created a portion of its website intended specifically for recruiters, which was available through a dedicated click tab labeled "recruiters" that was prominently displayed at the top of the Spokeo home page. Recruiters were encouraged to "Explore Beyond the Resume." In addition, Defendant promoted the Spokeo.com/HR URL to recruiters in the media and in marketing to third parties, and offered special subscription plans for its HR customers.

ln 2010, Spokeo changed its website Terms of Service to state that it was not a consumer reporting agency and that consumers may not use the company's website or information for FCRA-covered purposes. However, Spokeo failed to revoke access to or otherwise ensure that existing users, including subscribers who may have joined Spokeo through its Spokeo.com/HR page, or those who had previously purchased access to profiles through API user agreements, did not use the company's website or information for FCRA-covered purposes.

The consumer profiles Spokeo provides to third parties are "consumer reports" as defined [by the] FCRA . . . . Spokeo profiles are consumer reports because they bear on a consumer's character, general reputation, personal characteristics or mode of living and/ or other attributes listed in section 603(d), and are "used or expected to be used . . . in whole or in part" as a factor in determining the consumer's eligibility for employment or other purposes specified in section 604.

In providing "consumer reports" Spokeo is now and has been a "consumer reporting agency" ("CRA") as that term is defined in section 603(f) of the FCRA, 15 U.S.C. § 1681a(f). Spokeo regularly assembles "information on consumers"` into consumer reports that it provides to third parties in interstate commerce, including companies in the human/resources background screening, and recruiting industries. Defendant is in the business of furnishing consumer reports to third parties that are "used or expected to be used" for "employment purposes."

Section 607(3) of the FCRA requires CRAs to maintain reasonable procedures to limit the furnishing of consumer reports to the purposes specified in section 604, 15 U.S.C. § 1681b. These procedures require that the CRA, prior to furnishing a user with a consumer report, require the prospective users of the information to identify themselves to the CRA, certify the purpose for which the information is sought, and certify that the information will be used for no other purpose. The CRA must make a reasonable effort to verify the identity of each new prospective user and the uses certified prior to furnishing such user a consumer report. In addition, section 607(a) prohibits any CRA from furnishing a consumer report to any person it has reasonable grounds to believe will not use the consumer report for a permissible purpose. Spokeo has failed to maintain any procedures required by section 607(a).

Section 607(b) of the FCRA, 15 U.S.C. § 1681e(b), requires all consumer reporting agencies to follow reasonable procedures to assure maximum possible accuracy of consumer

report information Spokeo has failed to follow any reasonable procedures to assure maximum possible accuracy of the information in reports that it prepared as required by section 607(b).

Section 607(d) of the FCRA, 15 U.S.C. § 1681e(d), requires CRAs to provide a "Notice to Users of Consumer Reports: Obligations of Users Under the FCRA" ("User Notice") to any person to whom a consumer report is provided by the CRA. As required by section 607(d), the Commission has prescribed the content of the User Notice . . . . The User Notice provides users of consumer reports with important information regarding their obligations under the FCRA, including the obligation of the user to provide a notice to consumers who are the subject of an adverse action (e.g., denial of employment) based in whole or in part on information contained in the consumer report. Spokeo has failed to provide the section 607(d) User Notice to those who purchase consumer reports.

Section 604 of the FCRA, 15 U.S.C. § l681b, prohibits CRAs from furnishing consumer reports to persons who the consumer reporting agency does not have reason to believe have a "permissible purpose." Section 604(b), 15 U.S.C. § 1681b(b), includes employment purposes as a permissible purpose but prescribes certain conditions for furnishing and using consumer reports for employment purposes Spokeo regularly furnishes consumer reports to third parties without procedures to inquire into the purpose for which the user is buying the report. Spokeo has violated Section 604, 15 U.S.C. § 1681b, in furnishing consumer reports to persons that it did not have a reason to believe had a permissible purpose to obtain a consumer report.

Consent Decree and Order for Civil Penalties, Injunction and Other Relief

Plaintiff, the United States of America, . . . alleges that Defendant Spokeo, Inc. has engaged in violations of the Fair Credit Reporting Act and in unfair or deceptive acts or practices in violation of Section 5 of the Federal Trade Commission Act. The parties have agreed to entry of this Stipulated Final Judgment . . . to resolve all matters in dispute in this action without trial or adjudication of any issue of law or fact herein and without Defendant admitting the truth of, or liability for, any of the matters alleged in the Complaint.

IT IS ORDERED that:

Judgment in the amount of eight hundred thousand dollars ($800,000) is hereby entered against Defendant, as a civil penalty for violations of the FCRA pursuant to section 621(a) of the Fair Credit Reporting Act, 15 U.S.C. § 1681s(a).

Defendant agrees that the facts as alleged in the Complaint filed in this action shall be taken as true, without further proof, in any subsequent civil litigation filed by or on behalf of the Commission to enforce its rights to any payment or money judgment pursuant to this Order.

IT IS FURTHER ORDERED that Defendant [and affiliates] are hereby permanently restrained and enjoined from violating the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x, in particular:

1. Violating section 604 of the FCRA, 15 U.S.C. § 168lb, by furnishing a consumer report to any person who does not have a permissible purpose to receive the consumer report;

2. Failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to users that have a permissible purpose to receive them under section 604 of the FCRA, 15 U.S.C. § 1681b, as required by Section 607(a) of the FCRA, 15 U.S.C. § 1681e(a);

3. Failing to maintain reasonable procedures to assure the maximum possible accuracy of the information concerning the individual about whom a consumer report relates, as required by section 607(b) of the FCRA, 15 U.S.C. § 1681e(b); and

4. Failing to provide the "Notice to Users of Consumer Reports: Obligations of Users Under the FCRA" ("User Notice") required by section 607(d) of the FCRA, 15 U.S.C. § 1681e(d),

to all users of Defendant's consumer reports. *Provided, however,* that Defendant may provide an electronic copy of the User Notice to a user if: (a) in the ordinary course of business, the user obtains consumer report information from Defendant in electronic form, and (b) the notice is clear and prominent.

IT IS FURTHER ORDERED that Defendant make timely submissions to the Commission:

One year after entry of this Order, Defendant must submit a compliance report, sworn under penalty of perjury. Defendant must: . . . (c) describe in detail whether and how Defendant is in compliance with each Section of this Order; and (d) provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission;

For 20 years following entry of this Order, Defendant must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any designated point of contact; or (b) the structure of any entity that Defendant has any ownership interest in or directly or indirectly controls that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

IT IS FURTHER ORDERED that Defendant must create certain records for 20 years after entry of the Order, and retain each such record for five (5) years. Specifically, Defendant must maintain the following records: Accounting records . . . ; Personnel records . . . ; Copies of all training materials that relate to the collection and sale of consumer report information; Copies of all training materials that relate to Defendant's activities as alleged in the Complaint and Defendant's compliance with the provisions of this Order; All records and documents necessary to demonstrate full compliance with each provision of this Order . . . .

Notes

1. *Spokeo* is an example of what happens when a company unwittingly falls within the scope of a sectoral privacy law. Spokeo violated the FCRA by doing none of the things that an FCRA-covered entity was supposed to do. It was like they had never heard of the statute.
2. Spokeo still exists—it just includes a clear disclaimer that none of its data should be used for FCRA-covered purposes and it no longer markets itself to employers. In fact, every people-search engine of which I am aware works on the same basic model. When searching for myself on one of them I needed to check a box affirming that I would not use the data for any FCRA-covered purpose before receiving my report.
3. How good are these reports anyway? In some senses, quite good. These search engines have decent address information for most adults, though the attributed dates of residence are sometimes off. Phone numbers, email addresses, and criminal history information are more scattered, presumably because the websites are at the mercy of low-quality sources for some of that information. Also, many prominent people (Supreme Court Justices, members of Congress) have been delisted from the most easily accessible sites. When I searched in 2020, however, I was able to find home addresses for about half the Seventh Circuit judges.

Erickson v. First Advantage Background Services Corp., 981 F.3d 1246 (11th Cir. 2020)

Keith Erickson had his heart set on coaching his son's Little League team. He authorized a search of sex-offender records as part of his application, apparently without much worry—his record was entirely clean. To his surprise, he soon received a letter in the mail from First Advantage, the consumer reporting agency that performed the search. That letter brought unwelcome news: Erickson's name had returned a match. Though Erickson's own record was clear, his estranged father's was not. And because the two shared a name, the name-only search that Little League requested had flagged his father's record.

Erickson eventually sued First Advantage, claiming that the company's upsetting report failed to comply with the Fair Credit Reporting Act's "maximum possible accuracy" standard. The question for us is what that standard requires. The answer is that a report must be both factually correct and free from potential for misunderstanding. And because the report here met that standard, we affirm.

As we've already said, Keith Erickson signed up to serve as an assistant coach for his oldest son's Little League team—a role he had filled twice before. When he signed his application, Erickson authorized Little League to run a background check, which included a search of registered sex-offender records. He provided Little League with his name (at the time, Keith Dodgson), as well as his date of birth, social security number, and home address.

Little League passed this information on to First Advantage, a consumer reporting agency it had worked with for several years to obtain background reports on its applicants. According to its agreement with Little League, First Advantage enters applicants' information into its own database to search for matching criminal and sex-offender registry records. That database includes records and files purchased from Experian Public Records, Inc., which is yet another consumer reporting agency.

In a typical search for sex-offender records, First Advantage inputs an applicant's name, complete date of birth, and, if available, Social Security number. It is not uncommon for the database to contain a sex-offender registry record without the underlying record of conviction. And for some jurisdictions, including the one at play here, First Advantage's database (for reasons that are unclear and not challenged) only contains sex offenders' names and birth years, but not complete dates of birth. In an attempt to cast a broad net where information is incomplete, the Little League agreement specifies that First Advantage will search for sex-offender records using only an applicant's first and last name in any jurisdictions where the database lacks those complete dates of birth. And if one of those name-only searches returns a result, Little League in turn would need to review available demographic data from the relevant State's website before determining that a sex-offender record actually belongs to an applicant.

That brings us to the facts behind this case, none of which are in dispute. At the direction of Little League, First Advantage searched its database using Erickson's identifying information and did not find any matching criminal records. But it did find a sex-offender record: a "Keith Dodgson" in Pennsylvania. That match was obtained by a name-only search because the database did not include the sex offenders' complete dates of birth.

First Advantage prepared a background report on Erickson to send to Little League. After identifying the sex-offender record that matched Erickson's name, the report stated "This Record is matched by First Name, Last Name ONLY and may not belong to your subject. Your further review of the State Sex Offender Website is required in order to determine if this is your subject." The report then directed Little League to Pennsylvania's sex-offender data to compare the "demographic data and available photographs," noting that Little League might "conclude that the records do not belong to" Erickson.

First Advantage also sent Erickson a letter informing him that he "share[d] the same name with a known criminal or registered sex offender" and that the record would be sent to Little League for review. The letter noted that "Little League is aware this record may not be yours" and explained that Little League was "committed" to investigating further if it planned to deny Erickson's application based on the report. Finally, the report itself assured Erickson that if Little League planned to take "adverse action based in whole or in part on the contents of this report," it must first provide him with a copy of the report.

Any non-sex offender would likely feel worried after receiving that kind of report—but Erickson was devastated. He shared a name with his biological father, and though he had severed all contact years before, he knew that his father was the source of the match.

He went into damage control mode. Erickson called First Advantage to explain the situation, and his wife contacted Little League. A First Advantage representative explained that the match was based only on his name, and a Little League affiliate explained that this kind of thing "happens." Still, though it was unclear whether anyone at Little League had even seen the report yet, Erickson decided not to coach his son's team because of his humiliation.

To avoid further association with his father, Erickson and his wife decided to change their family's last name from Dodgson to Erickson—a decision that particularly stung Erickson, who had been known by his last name throughout his military career. What's more, military rules required him to disclose the reason for his name change to others in his chain of command, a process that he reports was painful. Erickson also made numerous disclosures to colleagues, neighbors, and friends about his father's status as a registered sex offender to explain why his family no longer went by the name "Dodgson."

Two months after receiving the sex-offender notification, Erickson initiated this lawsuit against First Advantage, alleging that the company failed to "follow reasonable procedures to assure maximum possible accuracy" of the information concerning Erickson in the report, in violation of the Fair Credit Reporting Act. 15 U.S.C. § 1681e(b). To succeed, Erickson needed to show both that First Advantage's report failed to comply with the Act's "maximum possible accuracy" standard and that the report caused him harm.

A jury trial followed. After he rested his case, First Advantage moved for judgment as a matter of law. The district court granted the motion, finding that Erickson had failed to establish two essential elements of his case: that the report was inaccurate and that it caused him harm. This appeal followed.

Before analyzing Erickson's "maximum possible accuracy" argument, we offer some background about the Fair Credit Reporting Act as a whole. One of the Act's stated purposes is to ensure fair and accurate reporting about consumers. 15 U.S.C. § 1681(a)–(b). To that end, it imposes various requirements on consumer reporting agencies. One of those requirements is that consumer reporting agencies "follow reasonable procedures" to ensure "maximum possible accuracy" of information in consumer reports. Consumers harmed when a consumer reporting agency fails to live up to that duty also have a private right of action under the Act.

We have previously explained that to make out a claim for a violation of § 1681e(b), a plaintiff must show at least two things: that a consumer report was inaccurate and that the inaccurate report caused him to suffer damages. And absent those showings—particularly the inaccurate report—the reasonableness of the reporting agency's procedures turns out not to matter. Here, the district court saw Erickson's case as doubly deficient—it concluded that the report to Little League was not "materially misleading" and that it did not damage Erickson in any event. Erickson of course disagrees.

This Court has not yet decided exactly what the "maximum possible accuracy" standard entails. We don't see why the Act should not be read to require that a report be both technically accurate and not misleading—in fact, we think that is what the statutory text demands. After all, the Fair Credit Reporting Act requires more than just accuracy in consumer reports—it requires "maximum possible accuracy." The words "maximum" and "possible" mean "greatest in quantity or highest in degree attainable" and "falling or lying within the powers" of an agent or activity. *Webster's Third New International Dictionary* 1396, 1771 (3d ed. 1961).

"Accuracy," in turn, means "freedom from mistake or error." *Webster's Third New International Dictionary* 13; *see also American Heritage Dictionary* 9 ("[e]xactness; correctness"). And being free from "mistake" or "error" means being free from "a misunderstanding of the meaning or implication of something" and not deviating from "truth or accuracy." *Webster's Third New International Dictionary* 772, 1446; *see also American Heritage Dictionary* 445, 840 (defining "mistake" as "error or fault" or a "misconception or

misunderstanding," and "error" as an "act, assertion, or belief that unintentionally deviates from what is correct, right, or true").

These definitions all point in one direction: that to reach "maximum possible accuracy," information must be factually true and also unlikely to lead to a misunderstanding. Under that standard, a report that contains factually incorrect information is plainly inaccurate under the Fair Credit Reporting Act. So too for a report that contains factually correct information but nonetheless misleads its users as to its meaning or implication.

Having defined the standard for "maximum possible accuracy," we now apply it. To begin, the Little League report was factually correct. The report stated that a registered sex offender in Pennsylvania shared Erickson's first and last name. True. And the report did not wrongfully attribute that record to Erickson. Closer to the opposite, in fact—it explained that the matching record was located using a name-only search and cautioned that the record might not be Erickson's at all.

Erickson says this is not enough. He argues that the report was "patently inaccurate": it was requested for him, it included a sex-offender record, and he is not a sex offender. But his conclusion just does not follow from his premises. The report never assigned the sex-offender record to Erickson, and again, it suggested that the record might *not* be connected to him. Simply put, the report was what it said it was—an alert that someone by the name of Keith Dodgson had a Pennsylvania sex-offender record.

That brings us to the second prong of the test—whether the report was misleading. And here, the only objectively reasonable interpretation of the report was one that was *not* misleading. A reasonable user of the report standing in the shoes of Little League—that is, a user who had hired a consumer reporting agency to search an internal database for sex-offender records, knowing that some searches would be performed only by name and knowing that further research was required before attributing any of those matched records to a particular individual—would not be misled by the report to such an extent that it would take negative action against Erickson. Little League knew that it would get what it asked for here—a search based only on first and last name. And it also knew that it could not attribute any of those matched records to an applicant without conducting further research first.

To be sure, this is not a license to caveat one's way out of liability for an affirmatively misleading report. We have all run into large-print headlines or promises that are belied by the lengthy fine print at the bottom. That kind of report would be objectively misleading. Nor will vague equivocations like "the criminal history cited may not be 100 percent accurate" suffice to save an otherwise misleading report. Some cases will be closer than this one, and require tighter judgment calls about whether a report is misleading. But here, the report's language made clear what the report was and was not, and it was prepared consistent with the expectations of the requester.

Notes

1. This case serves two useful purposes. First, it shows the breadth of reasons why reports such as these are commissioned. One would not normally think of Little League coaching as particularly related to "credit," yet this report falls neatly within the scope of the FCRA. Second, this shows the virtue of FCRA protections. One could easily imagine a first and last name match alone misleading an unwary searcher. But here we have a somewhat lawyerly clarification from First Advantage: note that this might *not* be the Keith that you are looking for. One could imagine the Little League having a brief moment of panic upon receiving this report and then being able to dispel its concern swiftly.
2. If we are to be fair to Keith, we also must ask why First Advantage did not do a better job here. It accurately reported the "just a name" match, but failed to recognize that it had sufficient information to discard the match. It is a failing of the First Advantage algorithm

that it did not consider the information it had on Keith Senior. The Eleventh Circuit is far from alone in not imposing greater burdens on consumer reporting agencies, however. The Seventh Circuit, Judge Easterbrook writing, pointed to the millions of records that Experian processes daily as a reason to not require it to actively check its records for internal consistency and instead rely on consumer complaints and feedback to identify errors. *Sarver v. Experian Info. Sols.*, 390 F.3d 969, 972 (7th Cir. 2004).

3. Is there a privacy harm here? Potentially yes. The report reveals to people who know Keith Jr. that Keith Sr. is a registered sex offender. This may damage Keith Jr.'s standing in the community even though it is not strictly speaking his secret. It also may have damaged Keith Sr.'s standing with his son and his son's community – it is unclear whether this report provided new information to that branch of the family – even though Keith Sr. was not a subject of the report.
4. Consumer reporting agencies often rely on public criminal record data to build the reports they sell, but this data is far from perfect and was often not intended to be used in this fashion. A study by Professor Sarah Lageson demonstrated that public criminal record data – as assembled by intermediaries – can incorrectly report an individual's criminal history, can be misleading as to the severity of the crimes committed and punishment imposed, and contain significant gaps in information due to administrative error. Furthermore, reporting agencies often do not verify or cross-check public records beyond basic name matches, leading to consumer reports that contain false positives (crimes where none were committed) and false negatives (no crime where some were committed).[181] So the "is this the right Keith" problem is quite common.

3) Federal Standing and FCRA claims

Claims under the Fair Credit Reporting Act can be brought in either state or federal court. Plaintiffs in federal court are required to have Article III standing. In general, standing requires that the plaintiff have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). In the context of privacy class actions, the main issue in dispute is whether there is an "injury in fact," which is why the construction of harm is so important.

The Supreme Court has been less than clear about what counts as an injury for standing purposes. In the 2016 *Spokeo* case, for instance, the Court held that "[t]o establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" The Court then clarified that "concreteness" and "particularity" are separate and distinct elements; a plaintiff must allege that his injury satisfies both for standing purposes.

In the context of privacy class action, particularization is not a major problem. A particular person's data is generally alleged to have been improperly collected or disclosed, so that particular person suffers a particularized harm. The particularity question has historically been most challenging in the environmental domain, where some injurious action might affect an entire community, or the entire country. The seminal particularity standing cases, *Lujan v. Defenders of Wildlife* 504 U.S. 555, 565–68 (1992) and *Friends of the Earth, Inc. v. Laidlaw Environmental Services* 528 U.S. 167, 180–81 (2000) both concerned environmental regulations.

[181] Sarah E. Lageson, *Criminal Data Function Creep*, 116 J. CRIM. L. & CRIMINOLOGY 113 (2026).

According to the Court, the challenge in those sorts of cases is to limit the right to sue to only those who are uniquely affected.[182]

Though particularity is not a major problem in the privacy domain, concreteness is often a serious issue.[183] The problem is that sometimes a legislature has granted an individual the ability to sue when some right is violated, but the courts are not sure whether the person has actually been hurt by the violation of that right. In his majority opinion in *Spokeo*, Justice Alito stated that Congress cannot grant a person a right to sue if that person has not been harmed, so courts will not defer entirely to legislative judgement.[184]

There is still some level of deference, however. Alito says the Court should find the conclusions of Congress instructive when considering whether a person has been harmed because Congress (or, presumably, a state legislature) is "well positioned to identify intangible harms." He then quotes Justice Kennedy's concurrence from *Lujan*, "Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before."

This semi-deference to legislative judgments about harm leads Justice Alito into a distinction between a "bare procedural violation" and actual harm.[185] When a legislature identifies actual harm, it can give a right to sue even though no right existed previously. But when the legislature establishes procedural rights, not every violation of those rights causes concrete harm. In the context of Fair Credit Reporting Act claims, for example, a consumer reporting agency may fail to follow procedural reporting requirements aimed at ensuring accuracy, a violation of the statute. If a plaintiff's credit report nonetheless remains accurate, however, they cannot establish concrete harm despite the consumer reporting agency's technical violation. Further, in Alito's view, not even all inaccuracies in credit reports cause concrete harms. An incorrect zip code in a credit report, for example, does not, "without more," "cause [concrete] harm or present any material risk of harm."

This set of distinctions between substantive and procedural harms puts courts facing issues of privacy and data security in an awkward position, as it is not always clear 1) when a procedural requirement serves a (sufficiently) substantive purpose that its violation qualifies as a harm and 2) when the violation of a procedural protection presents a material risk of harm. Take Justice Alito's example of an inconsequential inaccuracy: an incorrect zip code. Research has linked commute length to employee engagement and longevity, so employers sometimes consider commute length in hiring. This means that an incorrect zip code might indeed count against a job applicant; the prospective employer would misunderstand where they now live. Zip codes are also associated with the usual suite of demographic variables, including race and ethnicity, and zip code discrimination has been alleged in a variety of contexts.[186]

---

[182] *See* F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORNELL L. REV. 275, 279–89 (2008) (discussing the history of harms sufficient to confer standing).

[183] The way in which the concreteness requirement is applied in privacy cases arguably signals a meaningful shift in standing doctrine. Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 439 (2017) ("Whereas older standing cases focused on whether the plaintiff before the court was the right plaintiff, the newer privacy-based cases are focused on, or making assumptions about, whether or not the harm caused by the defendant is the right kind of harm.").

[184] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

[185] *Spokeo*, 136 S. Ct. at 1550.

[186] *See, e.g.*, NATIONAL FAIR HOUSING ALLIANCE, ZIP CODE INEQUALITY: DISCRIMINATION BY BANKS IN THE MAINTENANCE OF HOMES IN NEIGHBORHOODS OF COLOR (2014), https://nationalfairhousing.org/wp-content/uploads/2017/04/2014-08-27_NFHA_REO_report.pdf [https://perma.cc/78JT-8W4J].

Like Spokeo, the latest Supreme Court case on privacy standing came in the context of the Fair Credit Reporting Act. It is notable for its discussion of future harm and its general skepticism of procedural violations.

TransUnion LLC v. Ramirez, 594 U.S. 413 (2021)

Justice KAVANAUGH delivered the opinion of the Court

To have Article III standing to sue in federal court, plaintiffs must demonstrate, among other things, that they suffered a concrete harm. No concrete harm, no standing. Central to assessing concreteness is whether the asserted harm has a "close relationship" to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms including (as relevant here) reputational harm. *Spokeo, Inc.* v. *Robins* (2016).

In this case, a class of 8,185 individuals sued TransUnion, a credit reporting agency, in federal court under the Fair Credit Reporting Act. The plaintiffs claimed that TransUnion failed to use reasonable procedures to ensure the accuracy of their credit files, as maintained internally by TransUnion. For 1,853 of the class members, TransUnion provided misleading credit reports to third-party businesses. We conclude that those 1,853 class members have demonstrated concrete reputational harm and thus have Article III standing to sue on the reasonable-procedures claim. The internal credit files of the other 6,332 class members were *not* provided to third-party businesses during the relevant time period. We conclude that those 6,332 class members have not demonstrated concrete harm and thus lack Article III standing to sue on the reasonable-procedures claim.

In two other claims, all 8,185 class members complained about formatting defects in certain mailings sent to them by TransUnion. But the class members other than the named plaintiff Sergio Ramirez have not demonstrated that the alleged formatting errors caused them any concrete harm. Therefore, except for Ramirez, the class members do not have standing as to those two claims.

In 1970, Congress passed and President Nixon signed the Fair Credit Reporting Act. Three of the Act's requirements are relevant to this case. *First*, the Act requires consumer reporting agencies to "follow reasonable procedures to assure maximum possible accuracy" in consumer reports. § 1681e(b). *Second*, the Act provides that consumer reporting agencies must, upon request, disclose to the consumer "[a]ll information in the consumer's file at the time of the request." § 1681g(a)(1). *Third*, the Act compels consumer reporting agencies to "provide to a consumer, with each written disclosure by the agency to the consumer," a "summary of rights" prepared by the Consumer Financial Protection Bureau. § 1681g(c)(2).

The Act creates a cause of action for consumers to sue and recover damages for certain violations. The Act provides: "Any person who willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer" for actual damages or for statutory damages not less than $100 and not more than $1,000, as well as for punitive damages and attorney's fees. § 1681n(a).

Beginning in 2002, TransUnion introduced an add-on product called OFAC Name Screen Alert. OFAC is the U. S. Treasury Department's Office of Foreign Assets Control. OFAC maintains a list of "specially designated nationals" who threaten America's national security. Individuals on the OFAC list are terrorists, drug traffickers, or other serious criminals. It is generally unlawful to transact business with any person on the list. TransUnion created the OFAC Name Screen Alert to help businesses avoid transacting with individuals on OFAC's list.

When this litigation arose, Name Screen worked in the following way: When a business opted into the Name Screen service, TransUnion would conduct its ordinary credit check of the consumer, and it would also use third-party software to compare the consumer's name against

the OFAC list. If the consumer's first and last name matched the first and last name of an individual on OFAC's list, then TransUnion would place an alert on the credit report indicating that the consumer's name was a "potential match" to a name on the OFAC list. TransUnion did not compare any data other than first and last names. Unsurprisingly, TransUnion's Name Screen product generated many false positives. Thousands of law-abiding Americans happen to share a first and last name with one of the terrorists, drug traffickers, or serious criminals on OFAC's list of specially designated nationals.

Sergio Ramirez learned the hard way that he is one such individual. On February 27, 2011, Ramirez visited a Nissan dealership in Dublin, California, seeking to buy a Nissan Maxima. Ramirez was accompanied by his wife and his father-in-law. After Ramirez and his wife selected a color and negotiated a price, the dealership ran a credit check on both Ramirez and his wife. Ramirez's credit report, produced by TransUnion, contained the following alert: "***OFAC ADVISOR ALERT - INPUT NAME MATCHES NAME ON THE OFAC DATABASE." A Nissan salesman told Ramirez that Nissan would not sell the car to him because his name was on a "terrorist list." Ramirez's wife had to purchase the car in her own name.

The next day, Ramirez called TransUnion and requested a copy of his credit file. TransUnion sent Ramirez a mailing that same day that included his credit file and the statutorily required summary of rights prepared by the CFPB. The mailing did not mention the OFAC alert in Ramirez's file. The following day, TransUnion sent Ramirez a second mailing—a letter alerting him that his name was considered a potential match to names on the OFAC list. The second mailing did not include an additional copy of the summary of rights. Concerned about the mailings, Ramirez consulted a lawyer and ultimately canceled a planned trip to Mexico. TransUnion eventually removed the OFAC alert from Ramirez's file.

In February 2012, Ramirez sued TransUnion and alleged three violations of the Fair Credit Reporting Act. *First*, he alleged that TransUnion, by using the Name Screen product, failed to follow reasonable procedures to ensure the accuracy of information in his credit file. See § 1681e(b). *Second*, he claimed that TransUnion failed to provide him with *all* the information in his credit file upon his request. In particular, TransUnion's first mailing did not include the fact that Ramirez's name was a potential match for a name on the OFAC list. See § 1681g(a)(1). *Third*, Ramirez asserted that TransUnion violated its obligation to provide him with a summary of his rights "with each written disclosure," because TransUnion's second mailing did not contain a summary of Ramirez's rights. § 1681g(c)(2). Ramirez requested statutory and punitive damages.

Ramirez also sought to certify a class of all people in the United States to whom TransUnion sent a mailing during the period from January 1, 2011, to July 26, 2011, that was similar in form to the second mailing that Ramirez received. TransUnion opposed certification. The U. S. District Court for the Northern District of California rejected TransUnion's argument and certified the class.

Before trial, the parties stipulated that the class contained 8,185 members, including Ramirez. The parties also stipulated that only 1,853 members of the class (including Ramirez) had their credit reports disseminated by TransUnion to potential creditors during the period from January 1, 2011, to July 26, 2011. The District Court ruled that all 8,185 class members had Article III standing.

After six days of trial, the jury returned a verdict for the plaintiffs. The jury awarded each class member $984.22 in statutory damages and $6,353.08 in punitive damages for a total award of more than $60 million.

The "law of Art. III standing is built on a single basic idea—the idea of separation of powers." *Raines v. Byrd* (1997). Separation of powers "was not simply an abstract generalization

in the minds of the Framers: it was woven into the document that they drafted in Philadelphia in the summer of 1787." *INS v. Chadha* (1983).

Therefore, we start with the text of the Constitution. Article III confines the federal judicial power to the resolution of "Cases" and "Controversies." For there to be a case or controversy under Article III, the plaintiff must have a " 'personal stake' " in the case—in other words, standing. To demonstrate their personal stake, plaintiffs must be able to sufficiently answer the question: " 'What's it to you?' " Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 Suffolk U. L. Rev. 881, 882 (1983).

To answer that question in a way sufficient to establish standing, a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief. If "the plaintiff does not claim to have suffered an injury that the defendant caused and the court can remedy, there is no case or controversy for the federal court to resolve."

Requiring a plaintiff to demonstrate a concrete and particularized injury caused by the defendant and redressable by the court ensures that federal courts decide only "the rights of individuals," *Marbury v. Madison* (1803), and that federal courts exercise "their proper function in a limited and separated government," Roberts, *Article III Limits on Statutory Standing*, 42 Duke L. J. 1219, 1224 (1993). Under Article III, federal courts do not adjudicate hypothetical or abstract disputes. Federal courts do not possess a roving commission to publicly opine on every legal question. Federal courts do not exercise general legal oversight of the Legislative and Executive Branches, or of private entities. And federal courts do not issue advisory opinions. As Madison explained in Philadelphia, federal courts instead decide only matters "of a Judiciary Nature."

In sum, under Article III, a federal court may resolve only "a real controversy with real impact on real persons." *American Legion* v. *American Humanist Assn.* (2019).

The question in this case focuses on the Article III requirement that the plaintiff 's injury in fact be "concrete"—that is, "real, and not abstract." *Spokeo, Inc.* v. *Robins* (2016).

What makes a harm concrete for purposes of Article III? As a general matter, the Court has explained that "history and tradition offer a meaningful guide to the types of cases that Article III empowers federal courts to consider." *Sprint Communications Co. v. APCC Services, Inc.* 2008). And with respect to the concrete-harm requirement in particular, this Court's opinion in *Spokeo* v. *Robins* indicated that courts should assess whether the alleged injury to the plaintiff has a "close relationship" to a harm "traditionally" recognized as providing a basis for a lawsuit in American courts. That inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury. *Spokeo* does not require an exact duplicate in American history and tradition. But *Spokeo* is not an open-ended invitation for federal courts to loosen Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal courts.

As *Spokeo* explained, certain harms readily qualify as concrete injuries under Article III. The most obvious are traditional tangible harms, such as physical harms and monetary harms. If a defendant has caused physical or monetary injury to the plaintiff, the plaintiff has suffered a concrete injury in fact under Article III.

Various intangible harms can also be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion. And those traditional harms may also include harms specified by the Constitution itself.

In determining whether a harm is sufficiently concrete to qualify as an injury in fact, the Court in *Spokeo* said that Congress's views may be "instructive." Courts must afford due respect to Congress's decision to impose a statutory prohibition or obligation on a defendant, and to grant a plaintiff a cause of action to sue over the defendant's violation of that statutory prohibition or obligation. In that way, Congress may "elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." But even though "Congress may 'elevate' harms that 'exist' in the real world before Congress recognized them to actionable legal status, it may not simply enact an injury into existence, using its lawmaking power to transform something that is not remotely harmful into something that is." *Hagy v. Demers & Adams* (CA6 2018).

Importantly, this Court has rejected the proposition that "a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." *Spokeo*. As the Court emphasized in *Spokeo*, "Article III standing requires a concrete injury even in the context of a statutory violation."

Congress's creation of a statutory prohibition or obligation and a cause of action does not relieve courts of their responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III any more than, for example, Congress's enactment of a law regulating speech relieves courts of their responsibility to independently decide whether the law violates the First Amendment.

For standing purposes, therefore, an important difference exists between (i) a plaintiff's statutory cause of action to sue a defendant over the defendant's violation of federal law, and (ii) a plaintiff 's suffering concrete harm because of the defendant's violation of federal law. Congress may enact legal prohibitions and obligations. And Congress may create causes of action for plaintiffs to sue defendants who violate those legal prohibitions or obligations. But under Article III, an injury in law is not an injury in fact. Only those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that private defendant over that violation in federal court. As then-Judge Barrett succinctly summarized, "Article III grants federal courts the power to redress harms that defendants cause plaintiffs, not a freewheeling power to hold defendants accountable for legal infractions."

To appreciate how the Article III "concrete harm" principle operates in practice, consider two different hypothetical plaintiffs. Suppose first that a Maine citizen's land is polluted by a nearby factory. She sues the company, alleging that it violated a federal environmental law and damaged her property. Suppose also that a second plaintiff in Hawaii files a federal lawsuit alleging that the same company in Maine violated that same environmental law by polluting land in Maine. The violation did not personally harm the plaintiff in Hawaii.

Even if Congress affords both hypothetical plaintiffs a cause of action (with statutory damages available) to sue over the defendant's legal violation, Article III standing doctrine sharply distinguishes between those two scenarios. The first lawsuit may of course proceed in federal court because the plaintiff has suffered concrete harm to her property. But the second lawsuit may not proceed because that plaintiff has not suffered any physical, monetary, or cognizable intangible harm traditionally recognized as providing a basis for a lawsuit in American courts. An uninjured plaintiff who sues in those circumstances is, by definition, not seeking to remedy any harm to herself but instead is merely seeking to ensure a defendant's "compliance with regulatory law." Those are not grounds for Article III standing.[1]

As those examples illustrate, if the law of Article III did not require plaintiffs to demonstrate a "concrete harm," Congress could authorize virtually any citizen to bring a statutory damages suit against virtually any defendant who violated virtually any federal law. Such an expansive understanding of Article III would flout constitutional text, history, and precedent. In our view, the public interest that private entities comply with the law cannot "be

converted into an individual right by a statute that denominates it as such, and that permits all citizens (or, for that matter, a subclass of citizens who suffer no distinctive concrete harm) to sue."

A regime where Congress could freely authorize *unharmed* plaintiffs to sue defendants who violate federal law not only would violate Article III but also would infringe on the Executive Branch's Article II authority. We accept the "displacement of the democratically elected branches when necessary to decide an actual case." Roberts, 42 Duke L. J., at 1230. But otherwise, the choice of how to prioritize and how aggressively to pursue legal actions against defendants who violate the law falls within the discretion of the Executive Branch, not within the purview of private plaintiffs (and their attorneys). Private plaintiffs are not accountable to the people and are not charged with pursuing the public interest in enforcing a defendant's general compliance with regulatory law.

In sum, the concrete-harm requirement is essential to the Constitution's separation of powers. To be sure, the concrete-harm requirement can be difficult to apply in some cases. Some advocate that the concrete-harm requirement be ditched altogether, on the theory that it would be more efficient or convenient to simply say that a statutory violation and a cause of action suffice to afford a plaintiff standing. But as the Court has often stated, "the fact that a given law or procedure is efficient, convenient, and useful in facilitating functions of government, standing alone, will not save it if it is contrary to the Constitution." *Chadha*. So it is here.

We now apply those fundamental standing principles to this lawsuit. We must determine whether the 8,185 class members have standing to sue TransUnion for its alleged violations of the Fair Credit Reporting Act. The plaintiffs argue that TransUnion failed to comply with statutory obligations (i) to follow reasonable procedures to ensure the accuracy of credit files so that the files would not include OFAC alerts labeling the plaintiffs as potential terrorists; and (ii) to provide a consumer, upon request, with his or her complete credit file, including a summary of rights.

A

We first address the plaintiffs' claim that TransUnion failed to "follow reasonable procedures to assure maximum possible accuracy" of the plaintiffs' credit files maintained by TransUnion. 15 U.S.C. § 1681e(b). In particular, the plaintiffs argue that TransUnion did not do enough to ensure that OFAC alerts labeling them as potential terrorists were not included in their credit files.

Assuming that the plaintiffs are correct that TransUnion violated its obligations under the Fair Credit Reporting Act to use reasonable procedures in internally maintaining the credit files, we must determine whether the 8,185 class members suffered concrete harm from TransUnion's failure to employ reasonable procedures.[5]

Start with the 1,853 class members (including the named plaintiff Ramirez) whose reports were disseminated to third-party businesses. The plaintiffs argue that the publication to a third party of a credit report bearing a misleading OFAC alert injures the subject of the report. The plaintiffs contend that this injury bears a "close relationship" to a harm traditionally recognized as providing a basis for a lawsuit in American courts—namely, the reputational harm associated with the tort of defamation.

We agree with the plaintiffs. Under longstanding American law, a person is injured when a defamatory statement "that would subject him to hatred, contempt, or ridicule" is published to a third party. TransUnion provided third parties with credit reports containing OFAC alerts that labeled the class members as potential terrorists, drug traffickers, or serious criminals. The 1,853 class members therefore suffered a harm with a "close relationship" to the harm associated with the tort of defamation. We have no trouble concluding that the 1,853 class members suffered a concrete harm that qualifies as an injury in fact.

TransUnion counters that those 1,853 class members did not suffer a harm with a "close relationship" to defamation because the OFAC alerts on the disseminated credit reports were only misleading and not literally false. TransUnion points out that the reports merely identified a consumer as a "*potential* match" to an individual on the OFAC list—a fact that TransUnion says is not technically false.

In looking to whether a plaintiff 's asserted harm has a "close relationship" to a harm traditionally recognized as providing a basis for a lawsuit in American courts, we do not require an exact duplicate. The harm from being labeled a "potential terrorist" bears a close relationship to the harm from being labeled a "terrorist." In other words, the harm from a misleading statement of this kind bears a sufficiently close relationship to the harm from a false and defamatory statement.

The remaining 6,332 class members are a different story. To be sure, their credit files, which were maintained by TransUnion, contained misleading OFAC alerts. But the parties stipulated that TransUnion did not provide those plaintiffs' credit information to any potential creditors during the class period from January 2011 to July 2011. Given the absence of dissemination, we must determine whether the 6,332 class members suffered some other concrete harm for purposes of Article III.

Publication is "essential to liability" in a suit for defamation. Restatement of Torts § 577, Comment *a*, at 192. And there is "no historical or common-law analog where the mere existence of inaccurate information, absent dissemination, amounts to concrete injury." *Owner-Operator*. Other Courts of Appeals have similarly recognized the "retention of information lawfully obtained, without further disclosure, traditionally has not provided the basis for a lawsuit in American courts," meaning that the mere existence of inaccurate information in a database is insufficient to confer Article III standing.

The standing inquiry in this case thus distinguishes between (i) credit files that consumer reporting agencies maintain internally and (ii) the consumer credit reports that consumer reporting agencies disseminate to third-party creditors. The mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm. In cases such as these where allegedly inaccurate or misleading information sits in a company database, the plaintiffs' harm is roughly the same, legally speaking, as if someone wrote a defamatory letter and then stored it in her desk drawer. A letter that is not sent does not harm anyone, no matter how insulting the letter is. So too here.

Because the plaintiffs cannot demonstrate that the misleading information in the internal credit files itself constitutes a concrete harm, the plaintiffs advance a separate argument based on an asserted *risk of future harm*. They say that the 6,332 class members suffered a concrete injury for Article III purposes because the existence of misleading OFAC alerts in their internal credit files exposed them to a material risk that the information would be disseminated in the future to third parties and thereby cause them harm. The plaintiffs rely on language from *Spokeo* where the Court said that "the risk of real harm" (or as the Court otherwise stated, a "material risk of harm") can sometimes "satisfy the requirement of concreteness."

To support its statement that a material risk of future harm can satisfy the concrete-harm requirement, *Spokeo* cited this Court's decision in *Clapper*. But importantly, *Clapper* involved a suit for *injunctive relief*. As this Court has recognized, a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial.

But a plaintiff must "demonstrate standing separately for each form of relief sought." Therefore, a plaintiff 's standing to seek injunctive relief does not necessarily mean that the plaintiff has standing to seek retrospective damages.

TransUnion advances a persuasive argument that in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm. TransUnion contends that if an individual is exposed to a risk of future harm, time will eventually reveal whether the risk materializes in the form of actual harm. If the risk of future harm materializes and the individual suffers a concrete harm, then the harm itself, and not the pre-existing risk, will constitute a basis for the person's injury and for damages. If the risk of future harm does *not* materialize, then the individual cannot establish a concrete harm sufficient for standing, according to TransUnion.

Consider an example. Suppose that a woman drives home from work a quarter mile ahead of a reckless driver who is dangerously swerving across lanes. The reckless driver has exposed the woman to a risk of future harm, but the risk does not materialize and the woman makes it home safely. As counsel for TransUnion stated, that would ordinarily be cause for celebration, not a lawsuit. *Id.,* at 8. But if the reckless driver crashes into the woman's car, the situation would be different, and (assuming a cause of action) the woman could sue the driver for damages.

The plaintiffs note that *Spokeo* cited libel and slander *per se* as examples of cases where, as the plaintiffs see it, a mere risk of harm suffices for a damages claim. But libel and slander *per se* "require evidence of *publication*." And for those torts, publication is generally presumed to cause a harm, albeit not a readily quantifiable harm. As *Spokeo* noted, "the law has long permitted recovery by certain tort victims *even if their harms may be difficult to prove or measure*." But there is a significant difference between (i) an actual harm that has occurred but is not readily quantifiable, as in cases of libel and slander *per se*, and (ii) a mere risk of future harm. By citing libel and slander *per se*, *Spokeo* did not hold that the mere risk of future harm, without more, suffices to demonstrate Article III standing in a suit for damages.

Here, the 6,332 plaintiffs did not demonstrate that the risk of future harm materialized—that is, that the inaccurate OFAC alerts in their internal TransUnion credit files were ever provided to third parties or caused a denial of credit. Nor did those plaintiffs present evidence that the class members were independently harmed by their exposure to the risk itself—that is, that they suffered some other injury (such as an emotional injury) from the mere risk that their credit reports would be provided to third-party businesses. Therefore, the 6,332 plaintiffs' argument for standing for their damages claims based on an asserted risk of future harm is unavailing.

Even apart from that fundamental problem with their argument based on the risk of future harm, the plaintiffs did not factually establish a sufficient risk of future harm to support Article III standing. As Judge McKeown explained in her dissent, the risk of future harm that the 6,332 plaintiffs identified—the risk of dissemination to third parties—was too speculative to support Article III standing. The plaintiffs claimed that TransUnion could have divulged their misleading credit information to a third party at any moment. But the plaintiffs did not demonstrate a sufficient likelihood that their individual credit information would be requested by third-party businesses and provided by TransUnion during the relevant time period. Nor did the plaintiffs demonstrate that there was a sufficient likelihood that TransUnion would otherwise intentionally or accidentally release their information to third parties. "Because no evidence in the record establishes a serious likelihood of disclosure, we cannot simply presume a material risk of concrete harm." (opinion of McKeown, J.).

Moreover, the plaintiffs did not present any evidence that the 6,332 class members even *knew* that there were OFAC alerts in their internal TransUnion credit files. If those plaintiffs prevailed in this case, many of them would first learn that they were "injured" when they received a check compensating them for their supposed "injury." It is difficult to see how a risk of future harm could supply the basis for a plaintiff 's standing when the plaintiff did not even know that there was a risk of future harm.

Finally, the plaintiffs advance one last argument for why the 6,332 class members are similarly situated to the other 1,853 class members and thus should have standing. The 6,332 plaintiffs note that they sought damages for the entire 46-month period permitted by the statute of limitations, whereas the stipulation regarding dissemination covered only 7 of those months. They argue that the credit reports of many of those 6,332 class members were likely also sent to third parties outside of the period covered by the stipulation because all of the class members requested copies of their reports, and consumers usually do not request copies unless they are contemplating a transaction that would trigger a credit check.

That is a serious argument, but in the end, we conclude that it fails to support standing for the 6,332 class members. The plaintiffs had the burden to prove at trial that their reports were actually sent to third-party businesses. The inferences on which the argument rests are too weak to demonstrate that the reports of any particular number of the 6,332 class members were sent to third-party businesses. The plaintiffs' attorneys could have attempted to show that some or all of the 6,332 class members were injured in that way. They presumably could have sought the names and addresses of those individuals, and they could have contacted them. In the face of the stipulation, which pointedly failed to demonstrate dissemination for those class members, the inferences on which the plaintiffs rely are insufficient to support standing.

In sum, the 6,332 class members whose internal TransUnion credit files were not disseminated to third-party businesses did not suffer a concrete harm. By contrast, the 1,853 class members (including Ramirez) whose credit reports were disseminated to third-party businesses during the class period suffered a concrete harm.

B

We next address the plaintiffs' standing to recover damages for two other claims in the complaint: the disclosure claim and the summary-of-rights claim. Those two claims are intertwined.

In the disclosure claim, the plaintiffs alleged that TransUnion breached its obligation to provide them with their complete credit files upon request. According to the plaintiffs, TransUnion sent the plaintiffs copies of their credit files that omitted the OFAC information, and then in a second mailing sent the OFAC information.

In support of standing, the plaintiffs thus contend that the TransUnion mailings were formatted incorrectly and deprived them of their right to receive information in the format required by statute. But the plaintiffs have not demonstrated that the format of TransUnion's mailings caused them a harm with a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts. In fact, they do not demonstrate that they suffered any harm *at all* from the formatting violations. The plaintiffs presented no evidence that, other than Ramirez, "a single other class member so much as *opened* the dual mailings," "nor that they were confused, distressed, or relied on the information in any way." The plaintiffs put forth no evidence, moreover, that the plaintiffs would have tried to correct their credit files—and thereby prevented dissemination of a misleading report—had they been sent the information in the proper format. Without any evidence of harm caused by the format of the mailings, these are "bare procedural violation[s], divorced from any concrete harmThat does not suffice for Article III standing.

For its part, the United States as *amicus curiae*, but not the plaintiffs, separately asserts that the plaintiffs suffered a concrete "informational injury" under several of this Court's precedents. We disagree. The plaintiffs did not allege that they failed to receive any required information. Moreover, the plaintiffs have identified no "downstream consequences" from failing to receive the required information. They did not demonstrate, for example, that the alleged information deficit hindered their ability to correct erroneous information before it was later sent to third parties. An "asserted informational injury that causes no adverse effects cannot satisfy Article III."

No concrete harm, no standing. The 1,853 class members whose credit reports were provided to third-party businesses suffered a concrete harm and thus have standing as to the reasonable-procedures claim. The 6,332 class members whose credit reports were not provided to third-party businesses did not suffer a concrete harm and thus do not have standing as to the reasonable-procedures claim. As for the claims pertaining to the format of TransUnion's mailings, none of the 8,185 class members other than the named plaintiff Ramirez suffered a concrete harm.

Justice THOMAS, with whom Justice BREYER, Justice SOTOMAYOR, and Justice KAGAN join, dissenting.

Article III vests "[t]he judicial Power of the United States" in this Court "and in such inferior Courts as the Congress may from time to time ordain and establish." § 1. This power "shall extend to *all* Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority." § 2 (emphasis added). When a federal court has jurisdiction over a case or controversy, it has a "virtually unflagging obligation" to exercise it.

The mere filing of a complaint in federal court, however, does not a case (or controversy) make. Article III "does not extend the judicial power to every violation of the constitution" or federal law "which may possibly take place." *Cohens v. Virginia* (1821). Rather, the power extends only "to 'a case in law or equity,' in which a *right*, under such law, is asserted."

Key to the scope of the judicial power, then, is whether an individual asserts his or her own rights. At the time of the founding, whether a court possessed judicial power over an action with no showing of actual damages depended on whether the plaintiff sought to enforce a right held privately by an individual or a duty owed broadly to the community. See *Spokeo, Inc.* v. *Robins* (2016) (THOMAS, J., concurring). Where an individual sought to sue someone for a violation of his private rights, such as trespass on his land, the plaintiff needed only to allege the violation. But where an individual sued based on the violation of a duty owed broadly to the whole community, such as the overgrazing of public lands, courts required "not only injuria [legal injury] but also damnum [damage]."

The principle that the violation of an individual right gives rise to an actionable harm was widespread at the founding, in early American history, and in many modern cases. *Havens Realty Corp. v. Coleman* (1982) ("[T]he actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing"). And this understanding accords proper respect for the power of Congress and other legislatures to define legal rights. No one could seriously dispute, for example, that a violation of property rights is actionable, but as a general matter, "[p]roperty rights are created by the State." *Palazzolo v. Rhode Island* (2001). In light of this history, tradition, and common practice, our test should be clear: So long as a "statute fixes a minimum of recovery ..., there would seem to be no doubt of the right of one who establishes a technical ground of action to recover this minimum sum without any specific showing of loss." T. Cooley, Law of Torts *271. While the Court today discusses the supposed failure to show "injury in fact," courts for centuries held that injury in law to a private right was enough to create a case or controversy.

Here, each class member established a violation of his or her private rights. The jury found that TransUnion violated three separate duties created by statute. All three of those duties are owed to individuals, not to the community writ large.

Were there any doubt that consumer reporting agencies owe these duties to specific individuals—and not to the larger community—Congress created a cause of action providing that "[a]ny person who willfully fails to comply" with an FCRA requirement "with respect to any *consumer* is liable to *that consumer*." § 1681n(a) (emphasis added). If a consumer reporting agency breaches any FCRA duty owed to a specific consumer, then that individual (not all consumers) may sue the agency. No one disputes that each class member possesses this cause

of action. And no one disputes that the jury found that TransUnion violated each class member's individual rights. The plaintiffs thus have a sufficient injury to sue in federal court.

The majority today, however, takes the road less traveled: "[U]nder Article III, an injury in law is not an injury in fact." No matter if the right is personal or if the legislature deems the right worthy of legal protection, legislatures are constitutionally unable to offer the protection of the federal courts for anything other than money, bodily integrity, and anything else that this Court thinks looks close enough to rights existing at common law.

This approach is remarkable in both its novelty and effects. Never before has this Court declared that legal injury is *inherently* insufficient to support standing. And never before has this Court declared that legislatures are constitutionally precluded from creating legal rights enforceable in federal court if those rights deviate too far from their common-law roots. According to the majority, courts alone have the power to sift and weigh harms to decide whether they merit the Federal Judiciary's attention. In the name of protecting the separation of powers, this Court has relieved the legislature of its power to create and define rights.

Even assuming that this Court should be in the business of second-guessing private rights, this is a rather odd case to say that Congress went too far. TransUnion's misconduct here is exactly the sort of thing that has long merited legal redress.

Were there any doubt about the facts below, we have the helpful benefit of a jury verdict. The jury found that "Defendant TransUnion, LLC willfully fail[ed] to clearly and accurately disclose OFAC information in the written disclosures it sent to members of the class." And the jury found that "Defendant TransUnion, LLC willfully fail[ed] to provide class members a summary of their FCRA rights with each written disclosure made to them." I would not be so quick as to recharacterize these jury findings as mere "formatting" errors.

And then there is the standalone harm caused by the rather extreme errors in the credit reports. The majority (rightly) decides that having one's identity falsely and publicly associated with terrorism and drug trafficking is itself a concrete harm. For good reason. This case is a particularly grave example of the harm this Court identified as central to the FCRA: "curb[ing] the dissemination of false information." And it aligns closely with a "harm that has traditionally been regarded as providing a basis for a lawsuit." Historically, "[o]ne who falsely, and without a privilege to do so, publishes matter defamatory to another in such a manner as to make the publication a libel is liable to the other," even though "no special harm or loss of reputation results therefrom." Restatement of Torts § 569, p. 165 (1938).

The question this Court has identified as key, then, is whether a plaintiff established "a degree of risk" that is "sufficient to meet the concreteness requirement." *Spokeo*. Here, in a 7-month period, it is undisputed that nearly 25 percent of the class had false OFAC-flags sent to potential creditors. Twenty-five percent over just a 7-month period seems, to me, "a degree of risk sufficient to meet the concreteness requirement." If 25 percent is insufficient, then, pray tell, what percentage is?

The majority deflects this line of analysis by all but eliminating the risk-of-harm analysis. According to the majority, an elevated risk of harm simply shows that a concrete harm is *imminent* and thus may support only a claim for injunctive relief. But this reworking of *Spokeo* fails for two reasons. First, it ignores what *Spokeo* said: "[Our opinion] does not mean ... that the risk of real harm cannot satisfy the requirement of concreteness." Second, it ignores what *Spokeo* did. The Court in *Spokeo* remanded the respondent's claims for statutory damages to the Ninth Circuit to consider "whether the ... violations alleged in this case entail a degree of risk sufficient to meet the concreteness requirement." The theory that risk of harm matters only for injunctive relief is thus squarely foreclosed by *Spokeo* itself.

But even setting aside everything already mentioned—the Constitution's text, history, precedent, financial harm, libel, the risk of publication, and actual disclosure to a third party—

one need only tap into common sense to know that receiving a letter identifying you as a potential drug trafficker or terrorist is harmful. All the more so when the information comes in the context of a credit report, the entire purpose of which is to demonstrate that a person can be trusted.

And if this sort of confusing and frustrating communication is insufficient to establish a real injury, one wonders what could rise to that level. If, instead of falsely identifying Ramirez as a potential drug trafficker or terrorist, TransUnion had flagged him as a "potential" child molester, would that alone still be insufficient to open the courthouse doors? What about falsely labeling a person a racist? Including a slur on the report? Or what about openly reducing a person's credit score by several points because of his race? If none of these constitutes an injury in fact, how can that possibly square with our past cases indicating that the inability to "observe an animal species, even for purely esthetic purposes, ... undeniably" is? *Lujan*; see also *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc* (2000) ("plaintiffs adequately allege injury in fact when they aver that they use the affected area and are persons for whom the aesthetic and recreational values of the area will be lessened" Had the class members claimed an aesthetic interest in viewing an accurate report, would this case have come out differently?

And if some of these examples do cause sufficiently "concrete" and "real"—though "intangible"—harms, how do *we* go about picking and choosing which ones do and which do not? I see no way to engage in this "inescapably value-laden" inquiry without it "devolv[ing] into [pure] policy judgment." *Sierra* (Newsom, J., concurring). Weighing the harms caused by specific facts and choosing remedies seems to me like a much better fit for legislatures and juries than for this Court.

Finally, it is not just the harm that is reminiscent of a constitutional case or controversy. So too is the remedy. Although statutory damages are not necessarily a proxy for unjust enrichment, they have a similar flavor in this case. TransUnion violated consumers' rights in order to create and sell a product to its clients. Reckless handling of consumer information and bungled responses to requests for information served a means to an end. And the end was financial gain. "TransUnion could not confirm that a single OFAC alert sold to its customers was accurate." Yet thanks to this Court, it may well be in a position to keep much of its ill-gotten gains.[9]

Ultimately, the majority seems to pose to the reader a single rhetorical question: Who could possibly think that a person is harmed when he requests and is sent an incomplete credit report, or is sent a suspicious notice informing him that he may be a designated drug trafficker or terrorist, or is *not* sent anything informing him of how to remove this inaccurate red flag? The answer is, of course, legion: Congress, the President, the jury, the District Court, the Ninth Circuit, and four Members of this Court.

Justice KAGAN, with whom Justice BREYER and Justice SOTOMAYOR join, dissenting.

. . . I add a few words about the majority's view of the risks of harm to the plaintiffs. In addressing the claim that TransUnion failed to maintain accurate credit files, the majority argues that the "risk of dissemination" of the plaintiffs' credit information to third parties is "too speculative." But why is it so speculative that a company in the business of selling credit

[9] Today's decision might actually be a pyrrhic victory for TransUnion. The Court does not prohibit Congress from creating statutory rights for consumers; it simply holds that federal courts lack jurisdiction to hear some of these cases. That combination may leave state courts—which "are not bound by the limitations of a case or controversy or other federal rules of justiciability even when they address issues of federal law,"—as the sole forum for such cases, with defendants unable to seek removal to federal court. By declaring that federal courts lack jurisdiction, the Court has thus ensured that state courts will exercise exclusive jurisdiction over these sorts of class actions.

reports to third parties will in fact sell a credit report to a third party? And in addressing the claims of faulty disclosure to the plaintiffs, the majority makes a set of curious assumptions. According to the majority, people who specifically request a copy of their credit report may not even "*open[ ]* " the envelope. And people who receive multiple opaque mailings are not likely to be "confused." And finally, people who learn that their credit files label them potential terrorists would not "have tried to correct" the error. Rather than accept those suppositions, I sign up with Justice THOMAS: "[O]ne need only tap into common sense to know that receiving a letter identifying you as a potential drug trafficker or terrorist is harmful."

Notes

1. As Thomas notes at the end of his dissent, state courts are not bound by the standing requirements of federal courts. So, when a cause of action can be brought in either state or federal court – as is often the case for claims against private parties – a defeat on federal standing may simply move the case from the federal system to the state system. This is not possible when one is suing the federal government, however, because it cannot be sued in state court.
2. Many scholars believe that *TransUnion* perpetuates and expands upon a fundamental error in doctrine. Daniel Solove and Danielle Citron, for example, argue that the Supreme Court's understanding of privacy harms is "cramped" and that *TransUnion* "has significantly undermined the effectiveness of many privacy laws. Through the standing doctrine, the U.S. Supreme Court essentially nullified a key enforcement component of many privacy laws—private rights of action."[187]
3. Some early empirical results suggest that *TransUnion* has not been fatal to privacy lawsuits.[188] In one study that examined standing decisions between the publication of *TransUnion* and the end of 2023, 60% (58 out of 96) of federal data breach lawsuits were found to have established an injury in fact, and all but two of those cases also established the other elements of Article III standing. Many federal district courts appeared to continue to rely on pre-*Transunion* circuit precedent, suggesting that they were not convinced that *TransUnion* had drastically changed the legal landscape. The study did not explicitly examine the rate of standing dismissals prior to *TransUnion*, however, so it is unclear whether *Transunion* resulted in more dismissals overall.
   Notably, 12 of the 96 cases in that study were originally filed in state court and later removed to federal court by defendants. In 6 of these, the defendant raised the issue of standing in a motion to dismiss, something of an oddity given that the removing party has the burden to demonstrate that standing exists.[189] In 3 others the court raised the issue of standing, and in the final 3 the plaintiffs raised the issue of standing in attempt to get the case remanded to state court.

[187] Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of TransUnion v. Ramirez* 101 B.U. L. Rev. Online 62 (2021)

[188] Noelle Wilson & Amanda Reid, *Intangible Harms, Tangible Consequences: Analyzing the Impact of* TransUnion *on Standing to Sue for Data Breach,* 90 MISSOURI LAW REVIEW 477 (2025).

[189] For more on the issue of defendants removing and then seeking dismissal for lack of standing, see Zachary D. Clopton & Alexandra D. Lahav, *Fraudulent Removal*, 135 HARV. L. REV. F. 87 (2021).

IX. Consumer Privacy

A. Federal Trade Commission and Section 5 425
United States v. Easy Healthcare Corp., Case No. 1:23-cv-3107 (N.D. Ill. 2023) 426
United States v. Facebook, Inc. Case No. 19-cv-2184 (D.C. Dist. Ct. 2019) 432
In the Matter of Support King, LLC (SpyFone.com) (FTC 2021) 439
FTC v. Rite Aid Corp., No. 2:23-cv-5023 (E.D. Penn. 2023) 442
In the Matter of X-Mode Social, Inc. and Outlogic, LLC, C-4802 (FTC 2024) 448

B. Children's Privacy 456
1) Children's Online Privacy Protection Act 456
F.T.C. and N.Y. v. Google LLC and YouTube, LLC (D.D.C. 2019) 459
United States v. Epic Games, Inc. (E.D.N.C. 2022) 466
2) California Age-Appropriate Design Code Act 473
NetChoice, LLC v. Bonta, 170 F.4th 744 (9th Cir. 2026) 474

C. Marketing Privacy 485
1) CAN-SPAM Act 485
2) Telephone Consumer Protection Act 487

D. Tracking Privacy 487
1) ECPA and Online Tracking 487
In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589 (9th Cir. 2020) 487
2) Video Privacy Protection Act 495
In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 (3rd Cir. 2016) 495
Gardner v. Me-TV National Limited Partnership, 132 F.4th 1022 (7th Cir. 2025) 504

E. Biometric Privacy 506
Rosenbach v. Six Flags Entertainment Corporation, 129 N.E.3d 1197 (Ill. 2019) 508
Patel v. Facebook 932 F.3d 1264 (9th Cir. 2019) 513
Zellmer v. Meta, 104 F.4th 1117 (9th Cir. 2024) 519
Cothron v. White Castle System, Inc., 216 N.E.3d 918 (Ill. 2023) 525

F. Comprehensive State Privacy Laws 528
1) California Consumer Privacy Act 528
California v. Sephora USA, Inc. (Cal. Super. Ct. 2022) 533
American Honda Motor Co., No. ENF23-V-HO-2 (Cal. Privacy Prot. Agency, 2025) 537
California Delete Act 545
2) Other states 546

People adopt a multitude of identities throughout the day. They are parents, friends, workers, students, pedestrians, drivers, and co–passengers on the bus. In the eyes of businesses, however, they are most often consumers. People buy things. A large amount of American privacy law is therefore devoted to protecting the privacy of those who buy.

As you will see, privacy protections in this area are scattered. One legal regime protects children. Another unsuccessfully fights against spam emails. A third protects you from having Netflix tell people how many times you have rewatched Friends. Whenever Americans are identified as consumers, however, they are protected by the underfunded eye of the Federal Trade Commission.

A. Federal Trade Commission and Section 5

The Federal Trade Commission (FTC) has enforcement authority under a variety of privacy and data security statutes including the Gramm–Leach–Bliley Act, the Fair Credit Reporting Act, and the Children's Online Privacy Protection Act, and each of these statutes has considerable power within its narrow scope. In addition to those specific grants of authority, however, the FTC also has enforcement authority under Section 5 of the FTC Act (15 U.S.C. § 45). Section 5(a) of the FTC Act provides that "unfair or deceptive acts or practices in or affecting commerce, are . . . declared unlawful."

Though the Commission's jurisdiction under Section 5 is not without limit, it is broad. "The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions, . . . Federal credit unions, . . . common carriers, . . . [and] air carriers . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." FTC Act § 45(a)(2). In short, the FTC can use Section 5 to regulate anything that is not a bank, nonprofit, government entity, airline, or common carrier.

Further, the definitions of deceptive and unfair acts are broad as well. "Deceptive" practices are defined in the Commission's Policy Statement on Deception as involving a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances. An act or practice is "unfair" if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

These broad definitions are why the FTC is relevant to every facet of consumer privacy. Any action that deceives or harms consumers is arguably within the jurisdiction of the FTC under Section 5.

In addition, the Commission enforces a variety of other consumer protection statutes that prohibit specifically defined practices. These statutes generally specify that violations are to be treated as if they were "unfair or deceptive" acts or practices under Section 5. Many also provide that violations are to be treated as if they were violations of a trade regulation rule issued under Section 18 of the FTC Act (and thus subject to civil penalties).

Consent decrees. The FTC rarely litigates cases to trial and final judgment under Section 5. Most often, the FTC negotiates with the subject of a potential FTC complaint prior to the filing of the complaint, and then the complaint, proposed settlement, and consent decree are filed on the same day in federal court. This is why many of the below cases are presented in terms of complaint and settlement; there is no substantive discussion from a judge of the merits of the case. There is only that to which the parties have agreed.

Enforcement. There is no private right of action under Section 5, and the FTC can only seek injunctions for violations. This means that a company cannot receive a monetary fine the first time it is accused of violating Section 5 and settles with the FTC. The FTC is restricted to seeking injunctions in such cases. Common terms of such injunctions are:

A. Stop the specific allegations of deceptive and unfair acts or practices described in the complaint.
B. Avoid any future violations of Section 5.
C. Fund a 20-year monitoring program that produces regular reports to the FTC and allows it to supervise compliance with A and B.

Though these settlements do not include fines, they can be quite costly. The specific policy changes required by the FTC can involve the creation of entirely new data privacy or

data security programs or the shuttering of lucrative lines of business. And violating the settlement itself can lead to a new enforcement action—one that *can* lead to monetary fines. This second enforcement action would, of course, be aided by anything that was previously produced by the aforementioned monitoring program.

Nevertheless, some have argued that FTC enforcement under Section 5 falls short due to its lack of immediate monetary penalties. And, when penalties eventually come under a second enforcement action, they can often be too small relative to the magnitude and profitability of the misconduct. This is a critical issue in the *Facebook* case below.

The FTC's primary approach to privacy enforcement—at least up until the 2020s—was one of self-regulation and privacy policy enforcement. As explained by Daniel Solove and Woodrow Hartzog in their seminal piece on FTC privacy enforcement:

> At the urging of Congress in 1995, the FTC became involved with consumer privacy issues. The FTC initially encouraged self-regulation, which was justified by a fear that regulation would stifle the growth of online activity. Instead of the FTC creating rules, the companies themselves would create their own rules, and the FTC would enforce them. The FTC thus would serve as the backstop to the self-regulatory regime, providing it with oversight and enforcement—essentially, with enough teeth to give it legitimacy and ensure that people would view privacy policies as meaningful and trustworthy.

Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598–99 (2014). The same article also noted that the FTC's large breadth of statutory authority was not matched by a large amount of staffing. As of 2014, the FTC's Division of Privacy and Identity Protection had 46 staffers. And, to that date, the FTC had lodged about ten privacy-related complaints each year.

United States v. Easy Healthcare Corp., Case No. 1:23-cv-3107 (N.D. Ill. 2023)

Complaint for Permanent Injunction, Civil Penalty Judgment, and Other Relief

Plaintiff brings this action . . . to seek . . . permanent injunctive relief, civil penalties, and other relief for Defendant's acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and in violation of the Health Breach Notification Rule (the "Rule" or the "HBNR"), 16 C.F.R. § 318.

Defendant Easy Healthcare Corporation ("Defendant" or "Easy Healthcare") has developed, advertised, and distributed a mobile application ("app") called the Premom Ovulation Tracker ("Premom") that allows users to input and track various types of personal and health information. For example, users can log information about their periods and fertility and upload pictures of ovulation test strips that the app can analyze to attempt to predict the user's next ovulation cycle. Defendant also designed Premom to permit users to import their health data from other devices or apps.

Hundreds of thousands of women have downloaded and used Premom, giving Defendant access to their mobile phones and their health information and other personal data. Between 2017 and 2020, Defendant repeatedly and falsely promised Premom users in their privacy policies that Defendant: (a) would not share health information with third parties without users' knowledge or consent; (b) to the extent Defendant collected and shared any information, it was non-identifiable data; and (c) the data was used only for Defendant's own analytics or advertising. Further, its privacy policies over time promised that Defendant would otherwise notify and obtain consent from users before using its users' data for any other purposes.

These representations were false or deceptive. Since 2018, Defendant has shared Premom users' identifiable health information with Google, LLC ("Google") and marketing firm AppsFlyer Inc. ("AppsFlyer"). This sharing was contrary to Defendant's promises to users and

thus constitutes a breach of unsecured health information that requires notice to Premom users under the Health Breach Notification Rule. Because Defendant has not provided timely and proper notice to consumers, the FTC, or the media of this sharing, Defendant is in violation of the FTC Act and the Health Breach Notification Rule.

In addition to sharing users' sensitive health information with Google and AppsFlyer, between 2018 and 2020, Defendant shared users' sensitive, identifiable data with foreign mobile analytics companies Jiguang and Umeng. Defendant took no action to limit what these companies could do with their users' information. Rather, it merely agreed to each company's standard terms of service, all of which gave these companies broad latitude to use the data as they saw fit, including for advertising.

Defendant continued to share users' sensitive, identifiable data with Jiguang and Umeng, while promising privacy to its users, until the summer of 2020. At that time, the Google Play Store informed Defendant that its transfer of data to Umeng violated the Play Store policies, and separately the *Washington Post* reached out to Defendant for comment related to an article detailing their data practices.

In addition to making these false and deceptive representations to consumers, Defendant failed to implement reasonable privacy and data security measures. Because of these failures, Defendant shared Premom users' data with third parties in violation of Section 5 of the FTC Act and, and failed to provide notice to consumers, the FTC, and the media of a breach of unsecured health information in violation of the Health Breach Notification Rule.

THE PREMOM APP

Since at least 2017, Defendant has made Premom available to users for free download from the Apple App Store and the Google Play Store. In the product description on the Google Play Store, Defendant has described Premom as "the most accurate and reliable period tracker, ovulation calculator, and fertility calendar" and "the only fertility tracker and ovulation app that offers a pregnancy guarantee to help women who are trying to conceive (TTC) make their baby dreams come true." Hundreds of thousands of users have downloaded and used Premom.

Premom is designed to be used with ovulation test strips, which Easy Healthcare also produces and sells. Defendant's ovulation test kits have consistently ranked as a number one best seller on Amazon.com, and the test kits encourage purchasers to download the Premom app.

Defendant encourages women trying to conceive to upload pictures of ovulation tests and input large amounts of health information into the app. Premom's description in the Apple App Store states: "Track your symptoms and activities—period, moods, sex, sleep, cervix mucus, and more." Defendant further states in its Google Play Store description that "Our automatic ovulation test reader with ovulation test kits (OPK), offers optimized fertility predictions you can trust." For instance, while using the app, Premom asks users to input the dates they started their periods and upload results of progesterone tests.

In Premom's description in the Google Play Store and Apple App Store, Defendant further encourages women to connect Premom to third-party apps and products so that Premom can import health information from those apps or products. Specifically, Premom users can import their body temperatures, along with the date and time that the temperature is taken, from the Apple Health app. Users can also import their body temperatures from thermometers that connect to Premom via Bluetooth.

Through Premom, Defendant has collected extensive sensitive personal health information about consumers, including dates of menstrual cycles, temperatures, pregnancy and fertility status, whether and when pregnancies started and ended, weight, progesterone and other hormone results, and pregnancy-related symptoms. Defendant also tells users that

users can infer other facts about their health from this information, such as whether they suffer from conditions like Polycystic Ovary Syndrome or hormonal imbalances.

DEFENDANT MADE DECEPTIVE REPRESENTATIONS AND OMISSIONS ABOUT ITS INFORMATION COLLECTION, SHARING, AND USE PRACTICES

Since 2017, Defendant repeatedly falsely promised Premom users in their in-app and website privacy policies that Defendant (a) would not share health information with third parties; (b) to the extent Defendant collected and shared any information, it was non-identifiable data; and (c) the data was used only for Defendant's own analytics or advertising.

First, between April 2019 and September 2020, Defendant repeatedly stated in multiple in-app privacy policies that it would not share any health information with third parties without user consent. For example, in a privacy policy dated July 7, 2020, Defendant stated in a paragraph set off from other paragraphs: "WE PROMISE WE WILL NEVER SHARE YOUR EXACT AGE OR ANY DATA RELATED TO YOUR HEALTH WITH ANY THIRD PARTIES WITHOUT YOUR CONSENT OR KNOWLEDGE."

Second, since at least December 13, 2021, Defendant has stated in their in-app and website privacy policy that "Premom uses AppsFlyer, a mobile marketing platform based in the United States, to handle non-health Personal Data" and that "third party services do not have access to your health information through the Services unless you share that information directly with them."

Third, Defendant also represented that it would share only "non-identifiable data" with third parties. Between May 2017 and July 2020, Premom's privacy policy posted on its website represented that it collected and shared Premom users' "nonidentifiable information for purposes of tracking analytics of the usage of [its] application." Premom's privacy policy represented that its use of third-party analytics software and software development kits "identifies a user solely by IP address."

Fourth, when a user wanted to connect a Bluetooth thermometer to Premom, Defendant prompted users with the following statement: "Please allow Premom to access your location and turn on the GPS for Bluetooth so it can find your thermometer" and asked users to "Allow Premom to access this device's location?" However, Defendant did not disclose in this prompt that it shared Premom users' location information with third parties.

Finally, Defendant represented that Premom users' data would be used only for Defendant's own analytics and advertising. Between May 2017 and July 2020, the privacy policy posted on Premom's website stated that it collected users' data to "[c]ustomize, measure and improve our services, content and advertising," and to "[e]valuate your use, preferences and trends for our own internal statistical and analytical purposes which we may use for marketing purposes . . . ." Defendant further represented that it "will not use your personal information for any purposes, other than those outlined in" Defendant's privacy policy or terms of service.

As described below, each of these representations or omissions made by Defendant was false or misleading.

DEFENDANT SHARED PREMOM USERS' HEALTH INFORMATION THROUGH CUSTOM APP EVENTS

Defendant integrated into the Premom app software development tools, known as software development kits ("SDKs"), from numerous third-party marketing and analytics firms. These SDKs provide functions for Defendant, such as enabling Defendant to track and analyze Premom users' interactions with Premom. By integrating these SDKs into Premom, Defendant would transfer its app users' data to the publisher of each SDK.

In fact, Defendant has incorporated SDKs from Google and AppsFlyer into the Premom app and disclosed health information to them through "Custom App Events."

Defendant tracks "Standard App Events," which are records of routine app functions, such as launching or closing the app, as well as "Custom App Events," which are records of user-app interactions unique to Premom. For example, when a user uploads a picture of an ovulation test, Defendant records the user's interaction with that feature as a Custom App Event that is shared with Google and AppsFlyer.

Rather than giving its Custom App Events anonymous names, Defendant chooses descriptive titles that convey health information about Premom users. For example, when a user opens Premom's calendar and logs her fertility, Defendant records the Custom App Event as "Calendar/Report/LogFertility." And when a user logs and saves information related to her period, Defendant records the Custom App Event as "Log period-save." By sharing these Custom App Events with either AppsFlyer or Google, Defendant consequently conveyed information about users' fertility and pregnancies.

By including sensitive health information in the titles of the Custom App Events it has shared through third-party SDKs, Defendant has conveyed the health information of hundreds of thousands of users to these third parties for years. Through these SDKs, Defendant has also collected and shared Premom users' unique advertising or device identifiers. [T]hird parties can use device identifiers to track consumers across the internet and apps, and eventually—through their own lists or by using a third-party service—match these identifiers to an actual person. Ultimately, this could allow these third parties to associate these fertility and pregnancy Custom App Events to a specific individual.

Defendant's transfers of these Custom App Events directly contradict Defendant's statements in their privacy policies that it would not share health information with third parties without users' knowledge or consent.

DEFENDANT SHARED CONSUMERS IDENTIFIABLE INFORMATION WITH THIRD PARTIES

Despite their assertions between 2018 and 2020 that their analytics software "identifies a user solely by IP address" and that it shared only *non-identifiable data* with third parties, Defendant—through the use of SDKs—collected and shared more than IP addresses, including information that could be used to identify Premom's users and disclose to third parties that these users were utilizing a fertility app.

Over various time periods since 2018, Defendant has incorporated into Premom the SDKs of, *inter alia*, Umeng, a Chinese mobile app analytics provider owned by the Chinese technology conglomerate Alibaba, and Jiguang, a Chinese mobile developer and analytics provider. Specifically, Defendant integrated U-Share and JPush, the SDKs marketed by Umeng and Jiguang respectively, into Premom.

Through the U-Share SDK, Defendant shared social media account information of Premom users with Umeng. By incorporating U-Share into Premom and sharing Premom users' social account information to Umeng, Defendant shared sensitive data that identifies its users.

Furthermore, the U-Share and JPush SDKs collected extensive amounts of other identifiable data on Premom's users and transmitted it to Umeng and Jiguang, including: a) resettable identifiers such as Android ID and Android Advertising ID; b) non-resettable identifiers, such as: Hardware Identification (HWID) and International Mobile Equipment Identity (IMEI) numbers—which are a set of numbers and letters that are unique and identify a computer or mobile phone [and] router, Bluetooth, and Wi-Fi Media Access Control (MAC) addresses—which are unique numbers hardcoded to those devices; and c) precise geolocation information—including Global Positioning System (GPS) coordinates information.

Companies can track consumers across the internet and devices via these resettable and non-resettable identifiers. A company can use these identifiers to track a consumer across apps

and devices, and to collect other information about them that, in combination with these identifiers, can be used to identify particular individuals.

Through the use of matching lists or through third-party services, a third-party can link these identifiers to a real person. Many surveillance advertising businesses specialize in tracking consumers' devices, collecting information on consumers, and identifying the consumer behind the device using this data, as well as connecting that consumer to other devices. Non-resettable identifiers are particularly important to the surveillance advertising industry. So, if a consumer provides their name in connection with an app that collects such resettable and non-resettable identifiers, or logs in to a major platform that shares such identifying information, then a third-party surveillance company or data broker can connect such identifiers to a person's name or identifying information.

In addition, when device identifiers are associated with precise geolocation data, the data becomes even more identifiable. With only a few location signals and a device identifier, third parties can identify a consumer's home address and identify other sensitive information about consumers, such as a consumer's healthcare provider or place of work. As such, through data shared through an SDK, a third party may learn that the user associated with advertising ID X12345 and IMEI ABC6789 spends every evening at 123 Main St., and thereafter, the third party will know that Jane Doe uses Premom, a weight loss app, and a smoking cessation app, and lives at 123 Main St.

In addition to violating their promises to consumers, Defendant's contracts with Umeng and Jiguang and sharing of this information with Umeng and Jiguang violated Apple and Google policies. Jiguang disclosed in its privacy policy that Jiguang collected Wi-Fi MAC addresses and Defendant reviewed and agreed to Jiguang's privacy policy before incorporating the Jpush SDK. Both Apple and Google contractually prohibit application developers from correlating, or syncing, the device advertising identifier with other identifiers, and from allowing third parties to obtain the advertising identifier via the application. Apple specifically forbids the collection of non-resettable device identifiers. Similarly, Google's Developer Policies state that in order to "protect user privacy," the Android Advertising ID "must not be connected to personally-identifiable information or associated with any persistent device identifier . . . without explicit consent of the user" and it restricts "access to MAC addresses." Typically, only a privileged app (e.g., a pre-installed app) can have access to the Wi-fi MAC address. However, the Jpush SDK circumvented Android's privacy controls and exploited a known bug in order to acquire Premom users' Wi-fi MAC addresses.

When Defendant sought Premom users' permission to access their location in order to pair a Bluetooth thermometer, it failed to disclose that it collected and shared precise geolocation information with Umeng and Jiguang . . . . Nor did Defendant disclose that Umeng and Jiguang could use and transfer this information for their own purposes, such as third-party advertising.

DEFENDANT VIOLATED THE HEALTH BREACH NOTIFICATION RULE

Congress enacted the American Recovery and Reinvestment Act of 2009, which directed the FTC to promulgate a rule requiring vendors of personal health records and related entities that collect healthcare information to provide notice to consumers and the FTC following a breach of security.

Pursuant to Section 13407 of the American Recovery and Reinvestment Act of 2009, . . . a violation of the Rule constitutes an unfair or deceptive act or practice in violation of Section 5(a) of the FTC Act.

Among other things, the Rule requires vendors of personal health records ("PHR") and PHR related entities to notify U.S. consumers and the FTC, and in some cases, the media, if they experience a breach of security.

The Rule defines "breach of security" to mean "with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual." 16 C.F.R. § 318.2(a).

The Rule defines "personal health record" to mean "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." 16 C.F.R. § 318.2(d).

The Rule defines "PHR identifiable health information" to mean "'individually identifiable health information,' [which is defined as] information: (1) [t]hat is provided by or on behalf of the individual; and (2) [t]hat identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." 16 C.F.R. § 318.2(e).

The Rule defines "vendor of personal health records" to mean "an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains a personal health record." 16 C.F.R. § 318.2(j).

The Rule defines "unsecured" to mean with respect to PHR identifiable information, such information "that is not protected through the use of a technology or methodology specified by the Secretary of Health and Human Services in guidance issued under section 13402(h)(2) of the American Reinvestment and Recovery Act of 2009. This guidance specifies that PHR identifiable information is protected when such information is "rendered unusable, unreadable, or indecipherable to unauthorized individuals" using technology such as encryption.

Defendant is a vendor of personal health records under the Rule. Defendant offers Premom, which is a personal health record because Premom collects and receives PHR identifiable health information from multiple sources. Premom users input health information into the Premom app. Among other health information, a Premom user can upload a picture of an ovulation test, which Premom then analyzes to determine whether the user is ovulating. Premom also collects users' health and non-health information from Bluetooth thermometers or third-party apps; for instance, a user can import from Apple Health her temperature and the date and time the temperature was taken. Moreover, . . . Premom users manage and control the PHR identifiable health information held in the Premom app. Each individual Premom user decides whether to input health information into Premom and how many of Premom's functions and services she will utilize.

In numerous instances, beginning in at least 2017, Defendant, as "a vendor of personal health records," experienced "breaches of security" of more than 500 consumers' unsecured PHR identifiable health information through the disclosure, and subsequent acquisition of Custom App Event titles relaying such information, by third parties such as Google and AppsFlyer, without the authorization of Premom users. This PHR identifiable health information was unsecured. This information was transferred to third parties such as Google and AppsFlyer without the use of encryption or other means to render it unusable, unreadable, or indecipherable to unauthorized individuals because this information was sent as Custom App Event titles in plain text . . . .

Based on the facts and violations of law alleged in this Complaint, the FTC has reason to believe that Defendant is violating or is about to violate laws enforced by the Commission because, among other things, Defendant has shared PHR identifiable health information with third parties without obtaining Premom users' authorization. Defendant's violation of the Health Breach Notification Rule is ongoing. Defendant has not notified users, in accordance with the notification provisions of the Health Breach Notification Rule, that it breached the security of Premom users' PHR identifiable health information through Premom's unauthorized disclosures to Google and AppsFlyer.

Notes

1. As part of its settlement, Easy Healthcare paid a $100,000 civil penalty for violating the Health Breach Notification Rule. It was also:
    a) Permanently prohibited from sharing user personal health data with third parties for advertising;
    b) Required to obtain user consent before sharing personal health data with third parties for other purposes;
    c) Required to retain users' personal information for only as long as necessary to fulfill the purpose for which it was collected;
    d) Prohibited from making future misrepresentations about Easy Healthcare's privacy practices and required to comply with the HBNR notification requirements for any future breach of security;
    e) Required to seek deletion of data it shared with third parties;
    f) Required to send and post a consumer notice explaining the FTC's allegations and the settlement; and
    g) Required to implement comprehensive security and privacy programs that include strong safeguards to protect consumer data.
2. In many ways this is a prototypical FTC enforcement action. Easy Healthcare made a series of privacy promises. It had not been required to make these promises but, having made them, it was bound to them. Had Premom come with different privacy promises, it would have been legal for them to do most of what they were doing–shenanigans with app store policies set to the side.
3. This case also shows the power of linking data. Merely knowing that device ID X has installed a period tracking app provides little information. Knowing what else that device has installed, knowing that it is linked to a set of locations, beginning to tie it to names or social media accounts—that is real power.
4. The Health Breach Notification rule was, for a long time, not a major factor in privacy law. But it has seen new life since a review in 2020, with the first enforcement actions being brought in 2023. It applies to non-HIPAA covered health data that is collected by vendors of personal health records (PHR). PHR is defined to include individually identifiable health information created or received by a health care provider, and "health care providers" includes any entities that "furnish[ ] health care services or supplies." Because health app purveyors furnish health care services to their users through the mobile applications they provide, the information held in the app is PHR identifiable health information, and therefore many health app purveyors likely qualify as vendors of personal health records. The rule also describes a breach to mean either a traditional breach (data security/hacking) or other unauthorized disclosures. This is being used here to make Easy Healthcare a vendor of PHR and its nonconsensual disclosure breaches.

United States v. Facebook, Inc. Case No. 19-cv-2184 (D.C. Dist. Ct. 2019)

Complaint for Permanent Injunction, Civil Penalty Judgment, and Other Relief

Facebook operates a social-networking service through its website—www.facebook.com—and mobile applications. Those applications connect consumer users of Facebook's service, who each create a Facebook "profile" showing personal information, with "Friends" who also have Facebook accounts and profiles ("Friends" or "Facebook Friends"). Through its service, Facebook collects and maintains vast amounts of consumer information. As of 2018, Facebook had more than 2.2 billion monthly active users worldwide. Over one hundred million Americans use Facebook every day to share personal information, such as their real name, date of birth, hometown, current city, employer, relationship status, and spouse's name, as well as sensitive personal information, such as political views, sexual orientation, photos of minor children, and membership in health-related and other support groups.

Facebook's core business model monetizes user information by using it for advertising. Substantially all of Facebook's $55.8 billion in 2018 revenues came from advertising.

To encourage users to share information, Facebook promises users that they can control the privacy of their information through Facebook's privacy settings. However, through at least June 2018, Facebook subverted users' privacy choices to serve its own business interests.

Beginning at least as early as 2010, every Facebook user who installed an app ("App User") agreed to Facebook sharing with the third-party developer of the installed app both information about the App User and the App User's Facebook Friends. Facebook's default settings were set so that Facebook would share with the third-party developer of an App User's app not only the App User's data, but also data of the App User's Facebook Friends ("Affected Friends"), even if those Affected Friends had not themselves installed the app. Affected Friends could only avoid this sharing by finding and opting out of it via settings on Facebook's Applications page, which was located on Facebook's website and mobile applications, separate and apart from Facebook's Privacy Settings page. Third-party developers that received user and Affected Friend information could use that information to enhance the in-app experience or target advertising to App Users and their Affected Friends. In the wrong hands, user and Affected Friend data could be used for identity theft, phishing, fraud, and other harmful purposes.

In 2012, after an FTC investigation, Facebook settled allegations that its practice of sharing Affected Friends' data with third-party developers of apps was deceptive. The resulting Commission Order, among other things, prohibits Facebook from misrepresenting the extent to which consumers can control the privacy of their information, the steps that consumers must take to implement such controls, and the extent to which Facebook makes user information accessible to third parties.

In the wake of the FTC's initial investigation, Facebook retained the separate opt-out sharing setting on its Applications page, but it added a disclaimer to its Privacy Settings page, warning users that information shared with Facebook Friends could also be shared with the apps those Friends used. However, four months after the 2012 Order was finalized, Facebook removed this disclaimer—even though it was still sharing Affected Friends data with third-party developers and still using the same separate opt-out setting that undermined users' privacy choices before entry of the Commission Order.

At its F8 conference in April 2014, . . . Facebook announced that it would stop allowing third-party developers to collect data about Affected Friends. Facebook also told third-party developers that existing apps could only continue to collect Affected Friend data for one year, or until April 2015. But, after April 2015, Facebook had private arrangements with dozens of developers, referred to as "Whitelisted Developers," that allowed those developers to continue to collect the data of Affected Friends, with some of those arrangements lasting until June 2018.

At least tens of millions of American users relied on Facebook's deceptive privacy settings and statements to restrict the sharing of their information to their Facebook Friends, when, in fact, third-party developers could access and collect their data through their Friends' use of third-party developers' apps. Facebook knew or should have known that its conduct violated the 2012 Order because it was engaging in the very same conduct that the Commission alleged was deceptive in Count One of the original Complaint that led to the 2012 Order.

As a general practice, Facebook did not vet third-party developers before granting them access to consumer data; instead, developers simply had to check a box agreeing to comply with Facebook's policies and terms and conditions, including those designed to protect consumer information. This made Facebook's enforcement of its policies, terms, and conditions acutely important.

Facebook's enforcement of its policies, terms, and conditions, however, was inadequate and was influenced by the financial benefit that violator third-party app developers provided to Facebook. This conduct was unreasonable. Facebook never disclosed this disparate enforcement practice to the third-party assessor charged by the 2012 Order with assessing the implementation and effectiveness of Facebook's privacy program, nor did Facebook disclose its enforcement practices to the Commission in its biennial assessment reports mandated by the 2012 Order.

In addition to its violations of the 2012 Order, Facebook also engaged in deceptive practices in violation of Section 5(a) of the FTC Act. Between November 2015 and March 2018, Facebook asked its users to provide personal information to take advantage of security measures on the Facebook website or mobile application, including a two-factor authentication measure that encouraged provision of users' phone numbers. Facebook did not effectively disclose that such information would also be used for advertising.

Finally, in April 2018, Facebook updated its data policy to explain that Facebook would use an updated facial-recognition technology to identify people in user-uploaded pictures and videos "[i]f it is turned on," implying that users must opt in to use facial recognition. Contrary to the implication of this updated data policy, however, tens of millions of users who still had an older version of Facebook's facial-recognition technology had to opt out to disable facial recognition. This violated the 2012 Order by misrepresenting the extent to which consumers could control the privacy of their information used for facial recognition.

Around the time that it resolved the Original Complaint through the Commission Order in 2012, Facebook added a disclaimer to the top of its desktop Privacy Settings page stating, "You can manage the privacy of your status updates, photos, and information using the inline audience selector—when you share or afterwards. *Remember: the people you share with can always share your information with others, including apps.*" (emphasis added). Approximately four months after the Commission Order became effective, however, Facebook removed the disclaimer from the Privacy Settings page.

Facebook's new "Privacy Settings" page purported to allow users to restrict who could see their past and future posts. Facebook did not disclose anywhere on this page, or anywhere along the path that users would have had to take to reach the Privacy Settings page, that users who shared their posts with "Friends" or a "Custom" audience could still have those posts shared with any of the millions of third-party developers whose apps were used by their Friends.

As was the case before the Commission Order, Affected Friends who sought to opt out of such sharing—and to have their privacy choices honored—needed to locate and adjust settings located under the separate "Apps" tab. The Apps tab did not alert users that it linked to a page containing settings that users had to disable in order to have their privacy choices fully honored.

In December 2012, Facebook introduced "Privacy Shortcuts," which it touted as a privacy tool that helps users navigate "key settings." *[S]ee* . . . Exhibit D (May 22, 2014 Press Release) (describing Privacy Shortcuts as a "tool designed to help people make sure they are sharing with just the audience they want").

The Privacy Shortcuts tool also had privacy settings for posts that purported to allow users to restrict their posts to Friends . . . . However, Facebook did not disclose on the Privacy Shortcuts tool, or anywhere along the path that users took to reach this tool, that their non-public posts could be shared with third-party developers of Friends' apps.

The format of the Apps Settings page varied over time. However, at all times relevant to this Complaint, the "Apps others use" setting at the bottom of the page, separate and apart from the privacy settings for the apps the user installed . . . .

On the "Apps others use" setting, Facebook stated, "People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information people can bring with them."

This was Facebook's only representation on any of the settings pages informing users that third-party developers of Friends' apps could access and collect their Profile Information.

By default, all categories of Affected Friend data, except "Religious and political views" and "Interested in," were set to be shared with third-party developers who requested them.

During all times relevant to this Complaint, only a very low percentage of users opted out of this default setting.

Facebook was aware of the privacy risks posed by allowing millions of third-party developers to access and collect Affected Friend data for nearly two years before it changed the Graph API to remove third-party developers' access to that data. By August 2013, Facebook had decided to remove third-party developers' access to Affected Friend data. As an internal document explained:

> We are removing the ability for users to share data that belongs to their friends who have not installed the app. Users should not be able to act as a proxy to access personal information about friends that have not expressed any intent in using the app.

In September 2013, Facebook audited a set of apps to determine whether to revoke their data permissions. That audit revealed that over a 30-day period, the audited apps were making hundreds of millions of requests to the Graph API for a variety of data, including Affected Friends' work histories, photos, videos, statuses, "likes," interests, events, education histories, hometowns, locations, relationships, and birthdays.

In some instances, the apps called for data about Affected Friends in numbers that greatly exceeded the number of the apps' monthly active users. For example, one app highlighted in the audit made more than 450 million requests for data—roughly 33 times its monthly active users.

Indeed, the volume of data acquired by the audited apps led one Facebook employee to comment, "I must admit, I was surprised to find out that we are giving out a lot here for no obvious reason."

Even though Facebook acknowledged the data-privacy risks associated with the data access it gave to third-party developers, on numerous occasions, while determining whether to continue granting a particular developer access to user data, it considered how large a financial benefit the developer would provide to Facebook, such as through spending money on advertisements or offering reciprocal data-sharing arrangements.

At one point in 2013, for instance, Facebook considered whether to maintain or remove data permissions for third-party developers based on whether the developer spent at least $250,000 in mobile advertising with Facebook.

As internal Facebook documents explained, Facebook would contact apps spending more than $250,000 on advertising and ask them to confirm the need for the data they were accessing, while Facebook would terminate access for apps spending less than $250,000.

Other than requiring third-party developers to agree to Facebook's policies and terms when they registered their app with the Platform, however, Facebook generally did not screen the third-party developers or their apps before granting them access to vast amounts of user data through Graph API V1.

For example, while Facebook used an automated tool to check that apps had an active link to a privacy policy, it did not actually review the app's privacy policy to confirm that it, in fact, complied with Facebook's policies.

Similarly, Facebook routinely granted third-party developers broad permissions to access user and Affected Friend data without first performing any checks on whether such permissions were consistent with a Facebook Platform policy requiring that apps request only data necessary to run the app or to enhance the user's app experience.

The Platform Policies outlined a number of privacy obligations and restrictions, such as limits on an app's use of data received through Facebook, requirements that an app obtain consent for certain data uses, and restrictions on selling or transferring user data. For example, third-party developers were specifically prohibited from transferring, directly or indirectly, any data—including aggregate, anonymous, or derivative data—to any ad network or data broker.

According to Facebook, these policies ensured that users' personal information was disclosed only to third-party developers who agreed to protect the information in a manner consistent with Facebook's privacy program.

To enforce its Platform Policies, Facebook relied on administering consequences for policy violations that came to its attention after third-party developers had already received the data. But Facebook did not consistently enforce its Platform Policies. Rather, the severity of consequences that Facebook administered to third-party developers for violating the company's Platform Policies, and the speed with which such measures were effectuated, took into account the financial benefit that Facebook considered the developer to offer to Facebook, such as through a commercial partnership.

Count 1—Misrepresenting the Extent to Which Users Could Control the Privacy of Their Data and the Extent to Which Facebook Made User Data Accessible to Third Parties

During the period from December 2012 through April 2014, Facebook represented to consumers that they could control the privacy of their data by using desktop and mobile privacy settings to limit the information Facebook could share with their Facebook Friends, including those on the Privacy Settings page, inline settings, Privacy Shortcuts, and profile settings.

In fact, Facebook did not limit its sharing of consumer information with third-party developers based on those privacy settings.

Count 2—Misrepresenting the Extent to Which Users Could Control the Privacy of Their Data and the Extent to Which Facebook Made User Data Accessible to Third Parties

At the April 30, 2014, F8 Conference, Facebook publicly announced that it would no longer allow third-party developers to access Affected Friend data.

In addition, Facebook continued to represent to consumers that they could control the privacy of their data by using Facebook's desktop and mobile privacy settings to limit to their Facebook Friends the information Facebook could share, including those on the Privacy Settings page, inline settings, Privacy Shortcuts, profile settings, and Privacy Checkup.

In fact, Facebook continued to allow millions of third-party developers access to Affected Friend data for at least another year.

Additionally, Facebook did not limit its sharing of consumer information with third-party developers based on Facebook's desktop and mobile privacy settings, including those on the Privacy Settings page, inline settings, Privacy Shortcuts, profile settings, and Privacy Checkup.

Count 3—Misrepresenting the Extent to Which Facebook Made User Data Accessible to Third Parties

At the April 30, 2014, F8 Conference, Facebook announced that it would no longer allow third-party developers to access Affected Friend data.

On April 30, 2015, Facebook generally deprecated Graph API V1 so that it was no longer publicly available to third-party developers.

However, Facebook privately granted the Whitelisted Developers continued access to the capabilities of Graph API V1.

As a result, even after April 30, 2015, the Whitelisted Developers maintained access to the same Affected Friend data that Facebook had publicly announced in April 2014 was no longer available to third-party developers.

Count 4—Failure to Implement and Maintain a Reasonable Privacy Program

In its initial and biennial assessment reports, Facebook claimed it had implemented controls and procedures to address the privacy risks created by third-party developers' access to user data.

These controls did not include screening the third-party developers or their apps before granting them access to user data. Instead, Facebook relied on enforcing its Platform Policies.

Despite substantial reliance on its Platform Policies, however, Facebook did not consistently enforce those policies from 2012 to the present. Rather, the severity of consequences it administered to violators of the Platform Policies, and the speed with which it effectuated such measures, took into account the financial benefit the violator provided to Facebook.

Count 5—Misrepresenting the Extent to Which Users Could Control the Privacy of Their Data

During the period from April 2018 through the present, Facebook represented, expressly or by implication, to its users that they would have to "turn[ ] on" facial-recognition technology.

In fact, during this period, for users who still had the Tag Suggestions Setting, Facebook's facial-recognition technology was turned on by default unless the user opted out.

Count 6—Deceptive Practices Regarding Use of Covered Information Provided for Account Security

Facebook represented, directly or indirectly, expressly or by implication, that users' phone numbers provided for two-factor authentication would be used for security purposes and, in some instances, to make it easier to connect with Friends on Facebook.

Facebook failed to disclose, or failed to disclose adequately, that Facebook would also use phone numbers provided by users for two-factor authentication for targeting advertisements to those users.

Facebook's failure to disclose or disclose adequately the material information . . . is a deceptive act or practice.

The acts and practices of Facebook as alleged in this Complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

Notes

1. **Settlement**. Facebook agreed to pay a five billion dollar fine to resolve this complaint. It also agreed to a series of privacy reforms:

a) Facebook must conduct a privacy review of every new or modified product, service, or practice before it is implemented, and document its decisions about user privacy;
b) Facebook must exercise greater oversight over third-party apps, including by terminating app developers that fail to certify that they are in compliance with Facebook's platform policies or fail to justify their need for specific user data;
c) Facebook is prohibited from using telephone numbers obtained to enable a security feature (e.g., two-factor authentication) for advertising;
d) Facebook must provide clear and conspicuous notice of its use of facial recognition technology, and obtain affirmative express user consent prior to any use that materially exceeds its prior disclosures to users;
e) Facebook must establish, implement, and maintain a comprehensive data security program;
f) Facebook must encrypt user passwords and regularly scan to detect whether any passwords are stored in plaintext; and
g) Facebook is prohibited from asking for email passwords to other services when consumers sign up for its services.

2. Defenders of the Facebook settlement point to the unprecedented size of the fine, twenty times that of the next largest, and the ambitious privacy program that Facebook was required to adopt. But the settlement was approved by a 3-2 vote of the Commission, with two Commissioners filing dissents.

Dissenting Statement of Commissioner Rebecca Kelly Slaughter

Civil Penalty Amount

Five billion dollars represents an astronomical penalty compared to prior Commission settlements or to the financial position of most individuals and firms. In the context of Facebook's financial position and scope of violations, it is a substantially less significant sum. From the time of the original 2012 Facebook order to 2018, Facebook's gross annual revenue increased more than 1000% from $5 billion to over $55 billion. Its 2019 revenues indicate continued growth, posting first-quarter earnings of over $15 billion. Put another way, as of this year, Facebook brings in around $5 billion on a monthly basis.

My colleagues in the majority note that civil penalties have exceeded $5 billion only in instances of serious environmental disaster or widespread financial fraud. I believe that the injury to the public from damaging the integrity of our elections is as serious if not more serious than environmental and financial harms because it threatens the very systems that stand to protect Americans from those harms. Concern over this fact pattern should be bipartisan; the manipulative tactics weaponized in favor of a particular party in one election can just as easily be turned against it in the next.

Finally, we must consider the necessity of vindicating the FTC's authority. In this analysis, I do find past penalty amounts (in both absolute and relative terms) informative to a degree; we need to consider if our standard practice with regard to enforcing orders, including through negotiation of penalties, is effective in ensuring firms take their compliance obligations seriously. The facts in this case raise serious questions about the effectiveness of our prior civil penalty settlements. Facebook's alleged conduct *while under order* strongly suggests that resolutions of prior order-violation cases failed to provide an effective deterrent.

Data Collection and Sharing

Data collection and sharing limitations would provide the most significant disciplining effect on Facebook's data privacy practices. The order the Commission voted to accept does not impose any limitations on whether Facebook can transfer information to third parties or to other Facebook subsidiaries. Instead, the order requires Facebook to demand certain purpose and use certifications from third parties that request information, giving Facebook free rein to

maintain control over what constitutes a permissible purpose and use. In other words, if Facebook wants third parties to have certain data, it can permit that under its Platform Terms; if Facebook wants to withhold access to that data, it can do so. But there may be a gulf between what is good for Facebook and what is good for its users. I believe that the order itself should limit third-party data access to information necessary to provide or operate the product or service for which the third party is requesting the information—it should not just rely on Facebook's malleable developer standards.

Liability Release

By far my biggest concern with the terms of the settlement is the release of liability, in particular the commitment that the order resolves "any and all claims that Defendant, its officers, and directors, prior to June 12, 2019, violated the Commission's July 27, 2012 order." I am also uncomfortable with the inclusion of "officers and directors" in the release from "any [Section 5] claim known by the FTC."

I am concerned that a release of this scope is unjustified by our investigation and unsupported by either precedent or sound public policy. To the contrary, in every recent major federal settlement, if there was a liability release, it was cabined to the offenses described in the complaint. Facebook's course of conduct also strongly counsels against this expansive release. Hardly a week passes without a news story revealing some potentially illegal conduct by Facebook.

Notes

1. The dissent talks about the role of Facebook data in American elections, referencing the Cambridge Analytica scandal. In simple terms, researcher Aleksandr Kogan was hired by Cambridge Analytica to create a Facebook app quiz. People who took the quiz had both their data and that of their friends exposed, ultimately totaling 87 million affected people—70 million of who were from the United States. This data was then used by Cambridge Analytica to target ads in the 2016 presidential election. When news of this use of Facebook data was exposed, Facebook's market cap declined over 100 billion in a matter of days.

In 2021, the FTC cracked down on SpyFone, the maker of a phone monitoring application. The application was designed to secretly run in the background on a phone, recording all device activity (texts, emails, pictures, location, etc.). Though a person needed to have physical access to the target phone to install the application, the purpose of the program was to run stealthily, without the target phone's user being aware of it. The FTC alleged that making this software and distributing it without taking steps to ensure it was only used for lawful purposes was an unfair practice. Further, SpyFone represented that its own storage of this surveillance data would be secure, and it was not. SpyFone agreed to discontinue its surveillance applications as part of its settlement.

In the Matter of Support King, LLC (SpyFone.com) (FTC 2021)

Complaint

Respondents license, market, and sell various monitoring products and services, each of which allows a purchaser to monitor surreptitiously another person's activities on that person's mobile device (the "device user"). These types of surreptitious monitoring apps have been used by stalkers and domestic abusers to monitor their victims' physical movements and online activities, as well as to obtain their sensitive personal information without authorization.

Respondents offer or have offered various monitoring products and services with varying capabilities and costs for Android devices:

SpyFone for Android Basic: Respondents' SpyFone for Android Basic ("Android Basic") is marketed as a product to monitor children or employees. Android Basic first became

available in 2018, and is sold on a subscription basis for $99.95 for twelve months. Once installed, Android Basic captures and logs, among other things, the following: SMS messages; call history; GPS location and live location; web history; contacts; pictures; calendar; files downloaded on the device; and notifications. It gives purchasers the ability to block apps, receive an app usage report, and also claimed it could spoof text messages so that the purchaser can send text messages that appear to be coming from the monitored device.

SpyFone for Android Xtreme: Respondents' SpyFone for Android Xtreme ("Android Xtreme") is marketed as SpyFone's "most popular" product, and also as a tool to monitor children or employees. Android Xtreme first became available in 2018, and is sold on a subscription basis for $179.95 for three months, or $299.95 for twelve months. In addition to the functionality included with Android Premium, Android Xtreme includes, among other things, a key logger, and live screen viewing. It also includes the ability to remotely take pictures, record audio by turning on the device's microphone, record calls, and send the mobile device commands through SMS, such as commands to vibrate or ring the mobile device.

Installing the SpyFone products requires that the purchaser have physical access to the device. The products are not available through the Google Play store, and instead must be downloaded from Respondents' website. Purchasers of SpyFone Android products that require installation must take steps to bypass numerous restrictions implemented by the operating system or the mobile device manufacturer on the monitored mobile device. Among other things, SpyFone instructs purchasers to enable the monitored mobile device to allow downloads from "unknown sources" for certain versions of Android. Android warns users "[i]f you download apps from unknown sources, your device and personal information can be at risk. Your device could get damaged or lose data. Your personal information could be harmed or hacked." SpyFone also instructs the purchaser to "disable[] the verification of applications," a security setting that identifies potentially harmful applications by scanning what applications are on the mobile device.

Once the purchaser installs the SpyFone Android product, he or she does not need physical access to the monitored mobile device, and can remotely monitor the device user's activities from an online dashboard.

Despite stating in a disclaimer that its monitoring products and services are designed for monitoring children or employees, Respondents do not take any steps to ensure that purchasers use Respondents' monitoring products and services for such purposes.

The purported use of the monitoring products and services for employment or child-monitoring purposes is a pretext. Parents and employers would not typically want the monitoring product to spoof text messages from the device, a feature SpyFone marketed to its customers, or want to disable security measures on a mobile phone to install Respondents' Android monitoring products and services—particularly when doing so may void a warranty and weaken the mobile device's security. Many other monitoring products are available in the marketplace that do not carry these risks.

Device users who are surreptitiously monitored using Respondents' monitoring products and services cannot stop the monitoring because they do not know it is happening. In fact, Respondents instruct the purchasers on how to hide the SpyFone products and services on the mobile device so that device users are unaware they are being monitored.

Respondents' SpyFone monitoring products and services substantially injure device users by enabling purchasers to stalk them surreptitiously. Stalkers and abusers use mobile device monitoring software to obtain victims' sensitive personal information without authorization and monitor surreptitiously victims' physical movements and online activities. Stalkers and abusers then use the information obtained via monitoring to perpetuate stalking and abusive behaviors, which cause mental and emotional abuse, financial and social harm, and physical harm, including death.

Stalking victims experience financial loss both directly and indirectly. Directly, stalkers and abusers can use the information obtained through monitoring products and services to take over a victim's financial accounts, and redirect any (or all) funds to the stalker or abuser. Indirectly, victims experience financial loss through the costs associated with therapy or counseling, and moving away from an abuser.

Statement of Commissioner Rohit Chopra

Today, the Commission has proposed banning Support King, the operator of SpyFone, and its top executive, Scott Zuckerman, from marketing surveillance software to address severe misconduct related to their spying software scheme.

As alleged in the Commission's complaint, Support King licensed and marketed products where stalkers and other users were given instructions on how to install an app on another person's mobile device, allowing users to have unfettered access to their target's location, text messages, and more. The company also employed shoddy security protocols that led to unauthorized access of sensitive personal records. To top it off, the company lied to its users about how it was handling the intrusion.

Surveillance Ban

The Commission is seeking public comment on banning Support King and Scott Zuckerman from licensing, marketing, or offering for sale surveillance products. This is a significant change from the agency's past approach. For example, in a 2019 stalkerware settlement, the Commission allowed the violators to continue developing and marketing monitoring products.

In addition to the surveillance ban, affected individuals will receive notifications that someone may have been surreptitiously monitoring their mobile device, as well as information to seek help if they may be in danger. The Commission welcomes public comment on these provisions.

Criminal Law Enforcement

The FTC's proposed order in no way releases or absolves Support King or Scott Zuckerman of any potential criminal liability. While this action was worthwhile, I am concerned that the FTC will be unable to meaningfully crack down on the underworld of stalking apps using our civil enforcement authorities. I hope that federal and state enforcers examine the applicability of criminal laws, including the Computer Fraud and Abuse Act, the Wiretap Act, and other criminal laws, to combat illegal surveillance, including the use of stalkerware.

While certain applications of these laws have been concerning, I believe it would be appropriate for enforcers to use these laws to seek criminal sanctions against individuals and firms that facilitate human endangerment through surveillance and stalkerware.

Notes

1. The subsequent order required the defendants to stop selling their monitoring products and from creating more monitoring products in the future. They also were required to notify purchasers that it is illegal to monitor adults in this way without their permission and create a notification on monitored phones informing users that their phones may have been monitored. Defendants were also required to hire a third-party assessor to monitor their compliance going forward.
   After settling this complaint, SpyFone ceased operation. Since the settlement targeted Zuckerman personally, and therefore also businesses that he subsequently developed, the order remained in effect. Zuckerman petitioned to have the order vacated in June 2025, citing the closure of SpyFone and changing FTC priorities. The FTC rejected this petition in December 2025, claiming that the decree was intended to survive the end of SpyFone, that the continuing burden on Zuckerman was appropriate, and that the FTC's enforcement

priorities in this domain had not changed. The decree was signed by the only two then-serving FTC commissioners, Andrew Ferguson and Mark Meador.[190]

2. Someone using SpyFone's technology could easily find themselves in violation of a variety of laws. If the app is installed without the target person's consent, the user is intruding on the target person's seclusion, violating both the Wiretap Act and the Stored Communications Act, probably running afoul of state stalking laws, and definitely running afoul of the Computer Fraud and Abuse Act. It is practically a cybercrime issue spotter, with the correct answer being that they are guilty of everything. What, then, was the lawful use of this technology? According to the company, it could be used to monitor the behavior of children and employees.
3. Notably the consumers being protected against unfair acts or practices here are not the purchasers of the SpyFone products. The FTC is instead protecting those who are using phones monitored by SpyFone.

FTC v. Rite Aid Corp., No. 2:23-cv-5023 (E.D. Penn. 2023)

Complaint for Permanent Injunction and Other Relief

The FTC brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), which authorizes the FTC to seek . . . permanent injunctive relief and other relief for Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Rite Aid Corporation . . . operates thousands of retail pharmacy locations throughout the United States. These locations sell a wide variety of products, including prescription and non-prescription medicines, medical supplies, groceries, cosmetics, and personal care items.

From at least approximately October 2012 until July 2020, Rite Aid has used facial recognition technology in hundreds of its retail pharmacy locations to identify patrons that it had previously deemed likely to engage in shoplifting or other criminal behavior in order to "drive and keep persons of interest out of [Rite Aid's] stores." The technology generated alerts sent to Rite Aid's employees, including by email or mobile phone application notifications ("match alerts"), indicating that individuals who had entered Rite Aid stores were matches for entries in Rite Aid's watchlist database.

In whole or in part due to facial recognition match alerts, Rite Aid employees took action against the individuals who had triggered the supposed matches, including subjecting them to increased surveillance; banning them from entering or making purchases at the Rite Aid stores; publicly and audibly accusing them of past criminal activity in front of friends, family, acquaintances, and strangers; detaining them or subjecting them to searches; and calling the police to report that they had engaged in criminal activity. In numerous instances, the match alerts that led to these actions were false positives (i.e., instances in which the technology incorrectly identified a person who had entered a store as someone in Rite Aid's database).

As described in more detail below, Rite Aid failed to take reasonable measures to prevent harm to consumers from its use of facial recognition technology. Among other things, Rite Aid failed to consider or address foreseeable harms to consumers flowing from its use of facial recognition technology, failed to test or assess the technology's accuracy before or after deployment, failed to enforce image quality standards that were necessary for the technology

---

[190] *In re Support King, LLC (SpyFone.com),* FTC Docket No. C-4756, Commission Order Denying Petition to Reopen and Vacate or Modify FTC Consent Order (Dec. 8, 2025). The transformation of the FTC during the second Trump administration is beyond the scope of this book. Realistically, there is nothing I can say here besides that the FTC is in a considerable state of flux and that it is hard to know what its enforcement priorities will be in 2027 and beyond. It was notable to me, however, that the FTC was completely uninterested in letting Zuckerman off the hook.

to function accurately, and failed to take reasonable steps to train and oversee the employees charged with operating the technology in Rite Aid stores.

Rite Aid's failures caused and were likely to cause substantial injury to consumers, and especially to Black, Asian, Latino, and women consumers.

Rite Aid is the subject of a 2010 order previously issued by the FTC for alleged violations of Section 5(a) of the FTC Act. Rite Aid violated provisions in the 2010 Order requiring it to (1) implement and maintain a comprehensive information security program and (2) retain documents relating to its compliance with that provision. Specifically, Rite Aid routinely failed to use reasonable steps in selecting and retaining service providers capable of appropriately safeguarding personal information they received from Rite Aid; require service providers by contract to implement and maintain appropriate safeguards for personal information they received from Rite Aid; and maintain written records relating to its information security program. Furthermore, Rite Aid failed to produce documents relating to its compliance with the 2010 Order, including documents that contradict, qualify, or call into question its compliance.

RITE AID'S USE OF FACIAL RECOGNITION TECHNOLOGY

Rite Aid obtained its facial recognition technology from two third-party vendors that operated and supported the technology on Rite Aid's behalf and at its direction in retail stores. Rite Aid also contracted with one of its vendors to provide additional biometric technologies for use in Rite Aid distribution centers.

Most of the stores in which Rite Aid installed the technology were located in and around New York City; Los Angeles; San Francisco; Philadelphia; Baltimore; Detroit; Atlantic City; Seattle; Portland, Oregon; Wilmington, Delaware; and Sacramento, California.

Rite Aid did not inform consumers that it used facial recognition technology. Additionally, Rite Aid specifically instructed employees not to reveal Rite Aid's use of facial recognition technology to consumers or the media.

Rite Aid's Enrollment Practices

In connection with its use of facial recognition technology, Rite Aid created, or directed its facial recognition vendors to create, an enrollment database of images of individuals whom Rite Aid considered "persons of interest," including because Rite Aid believed the individuals had engaged in actual or attempted criminal activity at a Rite Aid physical retail location or because Rite Aid had obtained law enforcement "BOLO" ("Be On the Look Out") information about the individuals. Enrollments in the Rite Aid database included images of the individuals ("enrollment images") along with accompanying information, including, to the extent known, individuals' first and last names, individuals' years of birth, and information related to criminal or "dishonest" behavior in which individuals had allegedly engaged.

Rite Aid regularly used low-quality enrollment images in its database. Rite Aid obtained enrollment images by, among other methods, excerpting images captured via Rite Aid's closed-circuit television ("CCTV") cameras, saving photographs taken by the facial recognition cameras, and by taking photographs of individuals using mobile phone cameras. On a few occasions, Rite Aid obtained enrollment images from law enforcement or from media reports. In some instances, Rite Aid employees enrolled photographs of individuals' driver's licenses or other government identification cards or photographs of images displayed on video monitors.

Rite Aid trained store-level security employees to "push for as many enrollments as possible." Rite Aid enrolled at least tens of thousands of individuals in its database. It was Rite Aid's general practice to retain enrollment images indefinitely.

Rite Aid's Match Alert Practices

Cameras installed in Rite Aid's retail pharmacy locations that used facial recognition technology would capture or attempt to capture images of all consumers as they entered or moved through the stores ("live images"). Rite Aid's facial recognition technology would then compare the live images to the enrollment images in Rite Aid's database to determine whether the live image was a match for an enrolled individual.

When Rite Aid's facial recognition technology determined that a live image depicted the same person as an enrollment image, the technology generated a "match alert" that was sent to store-level employees' Rite Aid-issued mobile phones. As part of the comparison process, Rite Aid's facial recognition technology generated "confidence scores" or "confidence levels"—numerical values that expressed the system's degree of confidence that two images were of the same person. A higher score indicated a higher degree of confidence. Rite Aid's facial recognition technology generated a match alert when the confidence score associated with a match was above a certain threshold that was selected by Rite Aid in consultation with its vendors.

However, match alerts provided to the store-level employees generally did not include confidence scores, so the employees who operated Rite Aid's facial recognition technology generally did not know the score associated with a given match alert.

Generally, match alerts contained both the enrollment image and the live image, as well as Rite Aid's instruction as to the action that Rite Aid's employees should take if the individual entered the store. Rite Aid instructed employees to take the stated action if the employees believed the match to be accurate.

Rite Aid's enrollments were assigned different match alert instructions depending on the reason the individual was enrolled. These instructions included (a) "Approach and Identify," (ii) "Observe and Provide Customer Service," (iii) "Pharmacy Patient – Escort to Pharmacy," and (iv) "911 Alert" or "Potentially Violent – Notify Law Enforcement and Observe." For enrollments with the instruction "911 Alert," employees were told to "call 911 and notify [the police that] a potentially violent or dangerous subject has entered the store."

A majority of Rite Aid's facial recognition enrollments were assigned the match alert instruction "Approach and Identify," which meant employees should approach the person, ask the person to leave, and, if the person refused, call the police.

Rite Aid's facial recognition technology generated thousands of false-positive matches—that is, alerts that incorrectly indicated that a consumer was a "match" for an enrollment in Rite Aid's database of individuals suspected or accused of wrongdoing. Indeed, despite a general failure to record the accuracy or outcomes of match alerts, Rite Aid employees recorded thousands of false positive match alerts between December 2019 and July 2020. Other evidence of false-positive matches includes:

a) In numerous instances, Rite Aid's facial recognition technology generated match alerts that were likely false positives because they occurred in stores that were geographically distant from the store that created the relevant enrollment. For example, between December 2019 and July 2020, Rite Aid's facial recognition technology generated over 5,000 match alerts in stores that were more than 100 miles from the store that created the relevant enrollment.
b) Some enrollments generated high numbers of match alerts in locations throughout the United States. For instance, during a five-day period, Rite Aid's facial recognition technology generated over 900 match alerts for a single enrollment. The match alerts occurred in over 130 different Rite Aid stores (a majority of all locations using facial recognition technology) . . . . In multiple instances, Rite Aid employees took action, including asking consumers to leave stores, based on matches to this enrollment.

c) Between December 2019 and July 2020, Rite Aid's facial recognition technology generated over 2,000 match alerts that occurred within a short time of one or more other match alerts to the same enrollment in geographically distant locations within a short period of time, such that it was impossible or implausible that the same individual could have caused the alerts in the different locations.

In connection with deploying facial recognition technology in a subset of its retail pharmacy locations, Rite Aid has failed to take reasonable measures to prevent harm to consumers. Among other things, Rite Aid has:

a) Failed to assess, consider, or take reasonable steps to mitigate risks to consumers associated with its implementation of facial recognition technology, including risks associated with misidentification of consumers at higher rates depending on their race or gender;
b) Failed to take reasonable steps to test, assess, measure, document, or inquire about the accuracy of its facial recognition technology before deploying the technology;
c) Failed to take reasonable steps to prevent the use of low-quality images in connection with its facial recognition technology, increasing the likelihood of false-positive match alerts;
d) Failed to take reasonable steps to train or oversee employees tasked with operating facial recognition technology and interpreting and acting on match alerts; and
e) Failed to take reasonable steps, after deploying the technology, to regularly monitor or test the accuracy of the technology, including by failing to implement any procedure for tracking the rate of false positive facial recognition matches or actions taken on the basis of false positive facial recognition matches.

In significant part as a result of Rite Aid's conduct, as discussed above, Rite Aid's facial recognition technology has generated numerous false positive facial recognition match alerts.

As a result of these false-positive match alerts, Rite Aid subjected consumers to surveillance, removal from stores, and emotional and reputational harm, as well as other harms.

Failure to Consider and Address Risks to Consumers, Including Increased Risks Based on Race or Gender

Rite Aid failed to consider, assess, or take into account the likelihood of false- positive matches or the potential risks false-positive matches posed to consumers.

An internal presentation advocating expansion of Rite Aid's facial recognition program following Rite Aid's pilot deployment of facial recognition technology identified only a single risk associated with the program: "[m]edia attention and customer acceptance."

Rite Aid failed to assess or address any other risks to consumers, including risks that false-positive match alerts could lead to a restriction of consumers' ability to make needed purchases, severe emotional distress, reputational harm, or even wrongful arrest.

Rite Aid also failed to take steps to assess or address risks that its deployment of facial recognition technology would disproportionately harm consumers because of their race, gender, or other demographic characteristics.

The accuracies of facial recognition technologies often vary depending on the demographics, including the race and gender, of image subjects. In particular, many currently available facial recognition technologies produce more false-positive matches for Black or Asian image subjects compared to White image subjects. Likewise, many facial recognition technologies have higher error rates for women image subjects than for men.

In fact, match alerts occurring in stores located in areas where the plurality of the population was Black or Asian were significantly more likely to have low confidence scores than match alerts occurring in stores located in plurality-White areas. Similarly, match alerts to enrollments with typically feminine names (i.e., where the enrolled person was likely a woman) were significantly more likely to have low confidence scores than match alerts to enrollments with typically masculine names.

Match alerts with low confidence scores were more likely to be false positives than match alerts with high confidence scores. Nonetheless, Rite Aid did not modify its policies in light of these low-confidence-score match alerts.

Failure to Test or Assess Accuracy Before Deployment

Rite Aid failed to test or assess the technology's accuracy before deploying facial recognition technology from its two vendors. Rite Aid did not ask its first vendor for any information about the extent to which the technology had been tested for accuracy and did not obtain, review, or rely on the results of any such testing. In fact, in its contract with Rite Aid, the vendor expressly disclaimed the accuracy of the technology it provided . . . .

In addition to its failure to test or assess accuracy when contracting with its first vendor, Rite Aid also failed to test for accuracy during its pilot deployment of the facial recognition technology.

Failure to Enforce Image Quality Controls

Rite Aid regularly used low-quality enrollment images in connection with its facial recognition technology, increasing the likelihood of false-positive match alerts.

Rite Aid knew that using high quality images was important for the accuracy of its facial recognition technology. For instance, Rite Aid employees noted in an internal presentation about its facial recognition technology that "[h]igh quality digital photos of enrollees enhance[d] [the] number of hits." And Rite Aid's first vendor told Rite Aid that "The quality of the photos used for [facial recognition technology] is extremely important . . . . Without good quality photos, an enrollment is not useful."

However, Rite Aid often used images that fell short of Rite Aid's own image quality standards contributing to the rate of false-positive match alerts.

Failure to Train and Oversee Employees

Rite Aid's failure to appropriately train or oversee employees who operated facial recognition technology further increased the likelihood of harm to consumers.

Although it was Rite Aid's policy that its retail stores provide employees authorized to operate facial recognition technology with approximately one to two hours of training on its facial recognition system, in nearly all cases Rite Aid did not verify or obtain any record that employees had received the required training.

Moreover, Rite Aid's training materials were very limited and did not address the risks to consumers from using the technology. Rite Aid never provided any training to any employees, for example, about the limitations of facial recognition technology, how to evaluate the quality of live images to determine their value for comparison, how to compare facial images to determine whether they are a match, or the effects of various types of bias on the accuracy of facial comparisons by humans.

Failure to Monitor, Assess, or Test Accuracy of Results

Rite Aid failed to regularly monitor and assess the accuracy of the results of its facial recognition technology. Rite Aid failed to record outcomes of alerts or track false positives in order to assess the accuracy of its facial recognition technology.

The facial recognition technology that Rite Aid initially deployed did not include a mechanism to track outcomes and Rite Aid did not establish a procedure to track outcomes. Rite Aid later switched to a technology that included a mechanism to record the outcome of an alert. Although Rite Aid's policy required employees to "resolve" every match alert, Rite Aid did not enforce this policy. For example, between December 2019 and July 2020, Rite Aid employees failed to "resolve" approximately two thirds of all match alerts.

Rite Aid retained active enrollments in its database even after they generated numerous false-positive matches. [Citing three examples that are particularly egregious, each of which generated hundreds of false positives.]

RITE AID'S FACIAL RECOGNITION TECHNOLOGY PRACTICES CAUSED OR WERE LIKELY TO CAUSE SUBSTANTIAL CONSUMER INJURY

Rite Aid's facial recognition technology practices caused or were likely to cause substantial consumer injury by increasing the risk of false-positive match alerts.

As described above, Rite Aid's use of facial recognition technology was especially likely to result in false-positive matches for Black, Latino, Asian, and women consumers.

In numerous instances, Rite Aid's employees acted on match alerts that were false positives. As a result, numerous consumers were mistakenly identified as shoplifters or wrongdoers.

Rite Aid's actions in relying on facial recognition technology without addressing these risks caused or were likely to cause injury to consumers, including because Rite Aid employees:

a. surveilled and followed consumers around the store;

b. instructed consumers to leave Rite Aid stores and prevented them from making needed or desired purchases, including prescribed and over-the- counter medications and other health aids;

c. subjected consumers to unwarranted searches;

d. publicly and wrongly accused consumers of shoplifting, including, according to consumer complaints, in front of the consumers' coworkers, employers, children, and others; or

e. called the police to confront or remove the consumer.

Therefore, taking action based on a false-positive match alert potentially exposed consumers to risks including the restriction of consumers' ability to make needed purchases, severe emotional distress, reputational harm, or even wrongful arrest.

Consumers complained to Rite Aid that they had experienced humiliation and feelings of stigmatization as a result of being confronted by Rite Aid's employees based on false- positive facial recognition matches.

Moreover, some of the consumers enrolled in Rite Aid's database or approached by Rite Aid's employees as a result of facial recognition match alerts were children. For example, Rite Aid employees stopped and searched an 11-year-old girl on the basis of a false-positive facial recognition match. The girl's mother told Rite Aid that she had missed work because her daughter was so distraught by the incident.

Multiple consumers told Rite Aid that they believed the false-positive facial recognition stops were a result of racial profiling. One consumer wrote to Rite Aid: "I feel different from this experience when I walk into a store now it's weird. Before any of your associates approach someone in this manner they should be absolutely sure because the effect that it can [have] on a person could be emotionally damaging . . . . [E]very black man is not [a] thief nor should they be made to feel like one."

The harms outlined above are not outweighed by countervailing benefits to consumers or competition.

Count I: Unfair Facial Recognition Technology Practices

In numerous instances, . . . Defendants have used facial recognition technology in their retail stores without taking reasonable steps to address the risks that their deployment of such technology was likely to result in harm to consumers as a result of false-positive facial recognition match alerts.

Defendants' actions cause or have been likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

Therefore, Defendants' acts or practices as set forth in Paragraph 140 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a), (n).

Notes

1. The consent decree in this case banned Rite Aid from using facial recognition for at least five years and required Rite Aid to implement comprehensive safeguards to prevent these types of harm to consumers when deploying automated systems that use biometric information to track them or flag them as security risks. It also requires Rite Aid to discontinue using any such technology if it cannot control potential risks to consumers.
2. What to make of Rite Aid's program? At best it sounds "legal, but dumb." At worst, it sounds like a Section 5 violation. Why would this program be implemented with so few safeguards, and why continued for a decade? It presumably cost Rite Aid customers and drained goodwill while also burdening staff. Should we suspect that there were some benefits—perhaps shoplifters were deterred—or is this likely a case of corporate inertia?
3. This case shows something of the FTC's newer approach to privacy issues. Rite Aid did not promise consumers that it would not implement a flawed facial recognition system. In fact, Rite Aid did not disclose the system at all. This stands in contrast to the "look for and enforce privacy promises" approach that dominated FTC enforcement even a few years earlier.

In the Matter of X-Mode Social, Inc. and Outlogic, LLC, C-4802 (FTC 2024)

Complaint

The Federal Trade Commission, having reason to believe that X-Mode Social, Inc., a corporation, and Outlogic, LLC, a limited liability company (collectively, "Respondents"), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

On approximately May 25, 2021, Respondent X-Mode consummated a joint venture with Digital Envoy, Inc., in which X-Mode transferred its business and substantially all of its assets to its successor, Outlogic, and Outlogic became a wholly-owned subsidiary of Digital Envoy. Throughout this complaint, "X-Mode" is used to refer to the conduct of both X- Mode and Outlogic, as its successor in interest.

X-Mode is a location data broker that sells consumer location data to hundreds of clients in industries ranging from real estate to finance, as well as private government contractors. According to its marketing material, X-Mode is the "2nd largest U.S. location data company." X-Mode sells access to the location data in two forms.

First, X-Mode licenses to third parties raw location data tied to unique persistent identifiers. These third parties can then analyze and use the data for their own purposes, such as advertising or brand analytics, or provide access to the information for their own customers.

Typically, such raw location data includes a unique persistent identifier for the mobile device called a Mobile Advertiser ID ("MAID"), the latitude, longitude, and a timestamp of the observation. This raw location data is capable of matching an individual consumer's mobile device with the locations they visited. Until at least May 2023 X-Mode did not have any policies or procedures in place to remove sensitive locations from the raw location data sets it sold. X-Mode's data could, therefore, be used to identify the sensitive locations that individual consumers have visited.

Second, X-Mode also licenses "X-Mode audience segments" tied to MAIDs for use by third parties. X-Mode analyzes the location data it obtains and based on the locations and events visited by mobile devices, categorizes MAIDs into "audience segments" based on interests or characteristics purportedly revealed by the locations or events. X-Mode offers audience segments such as "Size Inclusive Clothing Stores," "Firehouses," "Military Bases," and "Veterans of Foreign Wars."

X-Mode predominantly collects consumer location data through third-party apps that incorporate Respondents' software development kit ("SDK"), which is a collection of app development tools that, among other things, requests access to the location data generated by a mobile device's operating system. If the device user allows access, the X-Mode SDK receives the device's precise latitude and longitude, along with a timestamp and other information about the device's operating system. This information is then passed on to X-Mode. In some circumstances, X-Mode obtains location data from app developers and publishers through other means, such as server-to-server transfers.

X-Mode incentivizes app developers to incorporate the X-Mode SDK into their apps by promising the app developers passive revenue for each consumer's mobile device that allows the SDK to collect their location data. The X-Mode SDK has been integrated into more than 300 apps, including games, fitness trackers, and religious apps.

In addition to collecting consumer location data through its SDK, X-Mode also purchases location data associated with MAIDs from data brokers and other aggregators. These third parties transfer data directly to X-Mode daily through various cloud storage structures.

X-Mode has also collected consumer location data associated with MAIDs from users of its own mobile apps, Drunk Mode and Walk Against Humanity.

X-Mode aggregates the location data—from its SDK, other data brokers, and, in the past, its own apps—and sells it to third parties. These third parties range from advertisers, software as a service (SaaS) companies, analytics firms, consulting firms, commercial and educational research organizations, and private government contractors.

Through its own apps, partner apps, and other data brokers, X-Mode daily has ingested over 10 billion location data points from all over the world. X-Mode advertises that this location data is 70% accurate within 20 meters or less.

X-Mode does not restrict the collection of location data from sensitive locations such as healthcare facilities, churches, and schools. X-Mode contractually restricts how its customers may use location data. For example, one such restriction is that its customers cannot:

> use the X-Mode Data (alone or combined with other data) to associate any user, device or individual with any venue that is related to healthcare, addiction, pregnancy or pregnancy termination, or sexual orientation, or to otherwise infer an interest or characteristic related to any of the foregoing

However, these contractual restrictions are insufficient to protect consumers from the substantial injury caused by the collection, transfer, and use of the consumers' location data from visits to sensitive locations.

X-Mode's Location Data Could Be Used to Identify People and Track Them to Sensitive Locations

X-Mode's location data associated with MAIDs could be used to track consumers to sensitive locations, including medical facilities, places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, and welfare and homeless shelters. For example, by plotting the latitude and longitude coordinates included in the X-Mode data stream using publicly available map programs, it is possible to identify which consumers' mobile devices visited medical facilities. Further, because each set of coordinates in X-Mode's data is time-stamped, it is also possible to identify when a mobile device visited the location.

The raw data provided by X-Mode to its customers is not anonymized. It is possible to use the geolocation data, combined with the mobile device's MAID, to identify the mobile device's user or owner. For example, some data brokers advertise services to match MAIDs with "offline" information, such as consumers' names and physical addresses.

Even without such services, however, location data could be used to identify people. The location data sold by X-Mode typically includes multiple timestamped signals for each MAID. By plotting each of these signals on a map, much can be inferred about the mobile device owners. For example, the location of a mobile device at night likely corresponds to the consumer's home address. Public or other records may identify the name of the owner or resident of a particular address.

X-Mode Failed to Honor Consumers' Privacy Choices

Since approximately 2013, the Android mobile phone operating system has included a privacy control that permitted users to "Opt out of Ads Personalization." This privacy control allows consumers to opt out from marketers using their phones' MAIDs to build profiles about the consumers or show the consumers personalized ads.

From approximately 2013 to 2021, when consumers enabled this control on their Android phones, the Android operating system would pass a phone's MAID to an app when requested by the app, along with other requested information, and would include a "flag" informing the app of the consumers' choice to opt out from personalized advertising.

From at least June 2018 to July 2020, X-Mode ingested the MAIDs, mobile location data, and flags of consumers who had enabled the "Opt out of Ads Personalization" control on their Android mobile phones, and, in many instances and contrary to these consumers' privacy choices, provided access to this data to marketers and other customers. X-Mode provided access to this data so that its customers could, among other things, build profiles about those consumers and serve them personalized advertising. During this time period, consumers were unaware that their privacy choices were not being honored by X-Mode.

From at least June 2018 to July 2020, X-Mode failed to employ the necessary technical safeguards and oversight to ensure that consumers' privacy choices enabled on their Android phones were honored and that their location data was no longer collected or sold for personalized advertising purposes.

X-Mode Failed to Notify Users of its Own Apps of the Purposes for which Their Location Data Would be Used

Although X-Mode primarily obtains its location data through third parties, X- Mode published two of its own apps (Drunk Mode and Walk Against Humanity) and has collected consumers' location data from those apps. As required by iOS and Android policies, X-Mode provided consumers with in-app explanations requesting permission to collect the consumers' location data and purporting to provide the uses for the information. X-Mode also published a

privacy notice on its website, purporting to provide consumers with information about the company's use of their personal information, including location data.

However, until at least August 2020, the notices provided by X-Mode directly to consumers failed to fully disclose the purposes for which consumers' location data would be used. For example, a notice displayed in X-Mode's "Drunk Mode" app used language suggesting that consumers' location data would be used solely for "ad personalization and location-based analytics including ad performance, market research, and traffic and health research":

> **Consent Notice**
>
> We hope you are enjoying Drunk Mode! We really appreciate your support. To fund our operation costs and development of new features, we collect and share mobile ad IDs and location data with third parties to help them conduct ad personalization and location-based analytics including ad performance, market research, and traffic and health research. By proceeding you agree to the processing of personal data as described in our partners' privacy notices. You can go to your device settings at any time to withdraw (or deny) your consent.

Likewise, in X-Mode's privacy policy published on or about May 17, 2020, X- Mode identifies "customers" with which X-Mode shares consumers' information:

> **With Our Customers:** We share information, including Advertising IDs, Location Information, Usage Data, and interest segments created using that information, with our customers. Our customers may include brands, data platforms, online advertising networks, and companies that perform research about consumer behavior, targeted or customized advertising, or human traffic patterns. You can learn more about our customers here.

While X-Mode's consumer notices disclosed certain commercial uses of consumer location data, X-Mode failed to inform consumers that it would be selling data to government contractors for national security purposes.

These facts would be material to consumers in deciding whether to use or grant location permissions to mobile apps. Consumers have expressed concern about the amount of personal information various entities—like advertisers, employers, or law enforcement—know about them and about how such entities use their personal data. Consumers are increasingly reluctant to share their personal information, such as digital activity, emails, text messages, and phone calls, especially without knowing which entities will receive it. Such collection and use imposes an unwarranted invasion into consumers' privacy.

X-Mode is aware that understanding the purposes for which their personal information is being collected is material to consumers. Indeed, when advising app publishers on ways to "prime" users to opt-in to the collection of their location data, X-Mode has informed app publishers, "Users are more likely to allow access when trying to complete a task that clearly needs location access."

By failing to fully inform consumers how their data would be used and that their data would be provided to government contractors for national security purposes, X-Mode failed to provide information material to consumers and did not obtain informed consent from consumers to collect and use their location data.

X-Mode Has Provided App Publishers with Deceptive Consumer Disclosures

X-Mode provides sample consumer notices to third-party app publishers that mislead consumers about the purposes for which their location may be used.

In most instances, X-Mode does not communicate directly with consumers. Rather, X-Mode obtains most of its location data from third parties, including app publishers. Android

and iOS policies require app publishers to get users' permission to collect their precise location information.

Because X-Mode obtains most of its location data from third party apps, the company relies on these third parties to obtain informed consumer consent to collect, use, or sell location data. X-Mode has provided third party app publishers incorporating its SDK with recommended language for consumer disclosures in both apps and privacy policies.

For example, one consumer consent notice that X-Mode provided to third-party app publishers stated that consumers' location data would be shared "with third parties to help them conduct ad personalization and location-based analytics:"

> **General Privacy Notice**
>
> We hope you are enjoying [APP NAME]! We really appreciate your support. To fund our operation costs and development of new features, we collect and share mobile ad IDs and de-identified location data with third parties to help them conduct ad personalization and location-based analytics including ad performance, market research, and traffic and health research. By proceeding you agree to the processing of personal data as described in our partners' privacy notices. You can go to your device settings at any time to withdraw (or deny) your consent.

This notice and other notices provided by X-Mode to third-party app publishers fail to fully inform consumers how their data would be used and that their geolocation data would be provided to government contractors for national security purposes.

X-Mode Fails to Verify that Third-Party Apps Notified Consumers of the Purposes for which Their Location Data Would be Used

In addition to providing app publishers and others with incomplete and misleading notices, X-Mode has failed to verify that third-party apps incorporating its SDK obtain informed consumer consent to grant X-Mode access to their sensitive location data.

Although X-Mode has tracked the language used by third party apps in consumer notices, X-Mode, in many cases, has not taken corrective actions based on any review of this language. As a result of this tracking, X-Mode is aware that apps provided consumers with deficient notices that did not adequately inform consumers how their data would be used and that their location would be provided to government contractors for national security purposes. However, X-Mode failed to instruct the third-party apps to correct the notices, failed to suspend or terminate its relationship with the third-party apps, and continued to use the data.

X-Mode Has Targeted Consumers Based on Sensitive Characteristics

As discussed above, X-Mode licenses audience segments, categories of MAIDs based on shared characteristics, for use by third parties. X-Mode has a catalogue of audience segments that it provides standard to the marketplace. The company also created custom audience segments for customers with special requests.

X-Mode has created custom audience segments that were based on sensitive characteristics of consumers. X-Mode licensed these custom audience segments to a third party for advertising or marketing purposes. Specifically, X-Mode entered into an agreement with a privately held clinical research company to license custom audience segments of consumers who had visited Cardiology, Endocrinology, or Gastroenterology offices and visited a pharmacy or drugstore in the Columbus, Ohio area and consumers that had visited a specialty infusion center. The purchase order from the organization explained the categorization and use as follows:

- X-Mode audiences will include the following panel sent to Licensee as a weekly feed:
    - Devices that have visited a cardiology, endocrinology, or gastroenterology office in Columbus, Ohio (list provided by Licensee and updated by X-Mode) AND that have visited a pharmacy/drugstore
        - Dwell time of 30min+
        - Time period of last 6 months initially and updated with last 7 days each week
        - Licensee has flexibility to adjust audience parameters, add venues, etc.
    - Devices that have visited a specialty infusion center (list provided by Licensee)
        - Dwell time of 1 hour+
        - Time period of last 6 months initially and updated with last 7 days each week
        - Licensee has flexibility to adjust audience parameters, add venues, etc.
- License Granted to X-Mode Data, and Applicable Restrictions. X-Mode hereby grants to Licensee a worldwide, term-limited (including the Wind-Down period set forth in Section 2(c)) license to access and use the X-Mode Data described above, to target ads for its own products or services through third party platforms

X-Mode's Business Practices Cause or are Likely to Cause Substantial Injury to Consumers

X-Mode's practices cause or are likely to cause substantial injury to consumers. For example, X-Mode's licensing agreements do not require their customers to employ reasonable and appropriate data security measures commensurate with the sensitivity of precise consumer location data, which increases the risk the information will be exposed in a data breach.

Further, X-Mode has little or no control over downstream uses of the precise location data that it sells. In fact, in at least two known instances, X-Mode sold location data to customers who violated contractual restrictions limiting the resale of such data. In such circumstances, X-Mode does not know the full extent of the exposure such as the identities of all third parties that received the data, how those third parties used the data, or whether those third parties further distributed the data to other recipients.

As described above, the data sold by X-Mode may be used to identify individual consumers and their visits to sensitive locations, such as visits to houses of worship and doctors' offices. The sale of such data poses an unwarranted intrusion into the most private areas of consumers' lives and causes or is likely to cause substantial injury to consumers.

For example, location data may be used to track consumers to places of worship, and thus reveal their religious beliefs and practices.

As another example, the location data could be used to track consumers who have visited women's reproductive health clinics and as a result, may have had or contemplated sensitive medical procedures such as an abortion or in vitro fertilization. Using the data X-Mode has made available, it is possible for third parties to target consumers visiting such healthcare facilities and trace that mobile device to a single-family residence.

Identification of sensitive and private characteristics of consumers from the location data sold by X-Mode is an invasion of consumers' privacy that causes or is likely to cause

substantial injury through loss of privacy, exposure to discrimination, physical violence, emotional distress, and other harms.

Additionally, the use of location data to categorize consumers based on sensitive characteristics causes or is likely to cause substantial injury. Such categorizations, particularly by companies that consumers never directly interact with, are far outside the expectations and experience of consumers, and can result in and cause additional injuries to consumers, including by exposing them to risks of discrimination.

The market for mobile location data is complex and typically opaque to consumers. Mobile location data, as electronically-stored information, is easily transferable and, as Respondents' practices demonstrate, may be sold and resold multiple times. Indeed, once the information is collected, many consumers lose the ability to control its use, spread, and retention, and therefore the harms described above are not reasonably avoidable by consumers.

These harms are not outweighed by any countervailing benefits to consumers or competition. X-Mode could implement certain safeguards at a reasonable cost and expenditure of resources. For example, X-Mode could audit the process by which its suppliers obtain consent and cease using location data that was not obtained with appropriate consent. Instead, X-Mode relies primarily on contractual language in supplier agreements requiring its suppliers to obtain appropriate consent from consumers and in data licensing agreements prohibiting misuse of its location data, but such language is insufficient to protect consumers from substantial injury. Moreover, even when X-Mode was aware that its suppliers were not obtaining appropriate consent, it continued to use consumers' location data provided by those suppliers.

Count I: Unfair Sale of Sensitive Data

Respondents sell, license, or otherwise transfer precise location data associated with unique persistent identifiers that reveal consumers' visits to sensitive locations, including, among others, locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters (such as shelters for the homeless, domestic violence survivors, or other at-risk populations), and addiction recovery.

This practice has caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. Consequently, this practice is an unfair act or practice.

Count II: Unfair Failure to Honor Consumer Privacy Choices

Respondents have collected and sold location data for the purposes of developing consumer profiles, surveilling consumers and targeting consumers with advertising even if consumers had opted-out of having their location data used for such purposes.

Count III: Unfair Collection and Use of Consumer Location Data

Respondents have collected consumers' location data from apps that Respondents owned without obtaining consumers' informed consent to the collection, use, or sale of their data.

Count IV: Unfair Collection and Use of Consumer Location Data Without Consent Verification

Respondents collect consumers' location data through third-party apps that incorporate Respondents' SDK without taking reasonable steps to verify that those consumers provide informed consent to the collection, use, or sale of their data.

Count V: Unfair Categorization of Consumers Based on Sensitive Characteristics for Marketing Purposes

Respondents have categorized consumers into audience segments based on sensitive characteristics, such as visits to medical offices derived from location data. They have sold these audience segments to a third party for marketing purposes.

Count VI: Deceptive Failure to Disclose Use of Location Data

[I]n numerous instances in connection with the collection, transfer, or sale of consumer location data, Respondents have represented, directly or indirectly, expressly or by implication, that Drunk Mode and Walk Against Humanity app users' location data would be used by third parties for ad personalization and location-based analytics including ad performance, market research, and traffic and health research purposes.

In fact, . . . Respondents have provided location data collected from Drunk Mode and Walk Against Humanity to government contractors for national security purposes. This fact would be material to consumers in deciding whether to use or grant location permissions to Respondents' apps.

Statement of Chair Lina M. Khan, on the X-Mode Consent Decree (Jan. 9, 2024)

Location data can reveal where someone lives, whom they spend time with, what medical treatments they seek, and where they worship. Of the many types of personal data, location data is among the most sensitive. Noting that "location records hold for many Americans the 'privacies of life,'" the Supreme Court held that constitutional safeguards against unchecked government surveillance extend to digital location tracking—even when the data is originally collected by private companies.

Americans deserve similar protection from unchecked corporate surveillance. Indeed, the explosion of business models that monetize people's personal information has resulted in routine trafficking and marketing of Americans' location data. As the FTC has stated, openly selling a person's location data to the highest bidder can expose people to harassment, stigma, discrimination, or even physical violence. And, as a federal court recently recognized, an invasion of privacy alone can constitute "substantial injury" in violation of the law, even if that privacy invasion does not lead to further or secondary harm.

The order secures notable relief, including a first-time ban on the use, sale, or disclosure of sensitive location data. The order also requires X-Mode to delete all the sensitive location data it has unlawfully collected, as well as any model, algorithm, or any other product derived in whole or in part from this unlawfully collected location data. X-Mode cannot collect, use, or disclose location data unless consumers have agreed to that. Finally, X-Mode must notify its customers of its deletion obligations under this order.

With this action, the Commission rejects the premise so widespread in the data broker industry that vaguely worded disclosures can give a company free license to use or sell people's sensitive location data.

Notes

1. To what standard is X-Mode being held? It variously is accused of:
   a. Collecting sensitive location data without consent.
   b. Collecting data from third-party apps without ensuring that those apps appropriately got consent.
   c. Collecting location data from their own apps without getting informed consent.
   d. Not honoring consumer privacy choices via the MAID flag in the Android operating system, and so ignoring the expressed preferences of users and their efforts to deny consent.

Of these, the last is the clearest problem; the flag set by users is an express rejection of consent. But what about the others? Was it clear that it was illegal to collect sensitive location data without consent? Is it clear now, after this complaint and settlement? How broadly or narrowly should we read this?

Key in the FTC's analysis appears to be the standards set not by the law, but by the policies of Android and iOS. On one hand, this seems strange. Why is the FTC suing for X-Mode's lack of adherence to its contract with two well-funded tech companies? But it makes a kind of sense from the consumer perspective. As a consumer, one is forced to put some trust in various companies. If Android and iOS tell me something about how my location data will be treated, I should be able to rely on it. Now it is possible that the FTC should also consider pursuing Google and Apple for not supervising their apps better, but it certainly makes sense to go after X-Mode for abusing what was supposed to be a safe-ish marketplace.

2. Another alleged problem was that the X-Mode privacy policies did not fully disclose the various things that X-Mode would do with location data. "While X-Mode's consumer notices disclosed certain commercial uses of consumer location data, X-Mode failed to inform consumers that it would be selling data to government contractors for national security purposes." Realistically, X-Mode consumers almost certainly do not read the privacy policy at all, let alone process it in that level of detail. So, what is the point of enforcing the policy? For years this question was at the heart of FTC privacy protection, as the contents of the privacy policy set the standard by which a company would be judged and, at the same time, everyone knew that consumers hardly ever read them. One of the good arguments for still taking privacy policies seriously is that other people read them. This results in headlines like "by sharing your location with ____ you are letting them ___." Not actively lying in a privacy policy is, in some sense, the bare minimum we can ask of a company.
3. Is it clear what location data is considered sensitive? Is the route of your daily run sensitive? Your weekly trip to the grocery store? Your visit to the movies?
4. The FTC's interest in location privacy continues after X-Mode. In 2026, the FTC settled with General Motors (GM) over its allegations that GM had used a misleading process to get consumers to sign up for its OnStar connected vehicle service and failed to clearly disclose that it collected precise geolocation data and sold it without user consent.[191] Under the terms of the settlement, GM was prohibited from sharing geolocation or driving behavior data with consumer reporting agencies for 5 years and from collecting covered driving data without affirmative express consent for 20 years. This was parallel to a California enforcement action.

B. Children's Privacy

1) Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act of 1998 (COPPA) applies to websites and online services under U.S. jurisdiction that are either directed at children under the age of thirteen or that have actual knowledge that they are collecting information from a child under the age of thirteen. 15 U.S.C. §§ 6501–6506. The FTC's implementing regulations are codified at 16 C.F.R. § 312.

General rule. An operator of a website or online service must obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including

[191] For further information, see this press release and the linked complaint and order: https://www.ftc.gov/news-events/news/press-releases/2026/01/ftc-finalizes-order-settling-allegations-gm-onstar-collected-sold-geolocation-data-without-consumers Notably, this order was approved by the Commission by a vote of 2-0, as there were only two active Commissioners by June of 2026.

consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

A website operator can collect a child's information without parental consent in highly limited circumstances. For instance, it can collect a guardian's contact information for use in asking for the guardian's consent. However, if the guardian refuses consent or does not reply, the operator must delete the information. The operator can also collect information to respond to a specific request from the child, if the interaction is a one-time affair and the operator makes reasonable efforts to inform the parents afterwards. There is also a narrow health and safety exception, allowing the collection to protect the safety of the child provided the information is not used for anything else.

Personal information. The term "personal information" means individually identifiable information about a child collected online, including: first and last name; home or other physical address including street name and name of city or town; online contact information or screen name (when it functions as contact information); telephone number; social security number; persistent identifier that can be used to recognize a user over time and across different websites or online services, such as a customer number held in a cookie, an internet protocol (IP) address, a processor or device serial number, or unique device identifier; photographs, videos, or audio containing a child's image or voice; and precise geolocation information. It is notable that this list includes persistent online identifiers and that it does not require combinations of data; an IP address is enough even if it is not associated with a name.

Collection. An entity has collected personal information from a child when it has requested, prompted, or encouraged the child to submit the information; when it has enabled the child to make personal information available in an identifiable form; or when it passively tracks the child.

Getting verified parental consent. The regulations list a host of acceptable mechanisms for getting verified parental consent including signed consent forms; requiring the parent to use a credit card; having the parent make a telephone call or video conference connection; and having the parent submit government-issued identification. The FTC allows vendors to submit proposals for new methods of obtaining parental consent and, if approved, use these functions as a safe harbor for operators. It keeps a public record of methods that have been approved or denied.[192] Notably, none of these methods are perfect. But they are legally sufficient.

Rights of parents/guardians. In addition to needing to give consent, parents and guardians are also given other rights under COPPA. They have the right to review the personal information collected from their child—without the process for doing so being unduly burdensome—and require its deletion. Notice to parents and guardians must also contain a description of what information the operator collects from children, including whether the website or online service enables a child to make personal information publicly available; how the operator uses such information; and the operator's disclosure practices for such information

Directed at children. When determining whether a website or online service, or a portion thereof, is directed to children, the FTC considers the subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The FTC will

[192] FEDERAL TRADE COMMISSION, VERIFIABLE PARENTAL CONSENT AND THE CHILDREN'S ONLINE PRIVACY RULE, https://www.ftc.gov/business-guidance/privacy-security/verifiable-parental-consent-childrens-online-privacy-rule.

also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.

A website or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another website or online service directed to children.

Data retention and security. An operator of a website or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator must also establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

Games and prizes. An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

Enforcement. COPPA can be enforced by the FTC and state attorney generals.

Notes

1.) Why does COPPA only apply to children under the age of thirteen? There is substantial tension between the desire to protect children during their formative years and the desire to allow them the freedom to grow as autonomous individuals. Is thirteen the right age? It allows the collection of information from high schoolers, but not middle schoolers. Note that parents can demand they be given information submitted by their children.

2.) What is the big deal with getting information from children? Is it really so bad if Amazon knows that this child likes Paw Patrol and that child likes Bluey? Are we worried about behavioral advertising, exploitation and physical threats, cultural corruption of the youth by online strangers, or all of the above?

3.) You, as an individual, likely cannot violate COPPA. Recall that these regulations apply to websites and online service providers collecting information from children. You can collect information from children in the offline context without violating COPPA. You can even distribute information about children online without violating COPPA, provided that you gathered that information in some other fashion.

4.) Many websites comply with COPPA by first, asking users their age or date of birth, and second, by not collecting information from anyone who reports being under the age of thirteen. Many underage users may lie about their age to pass these age gates, but their lies do not necessarily create problems for the website. Even if the website knows that many children lie, the website lacks "actual knowledge" of which children are lying.

5.) Asking users their ages without imposing such an age gate is extremely risky. This was demonstrated in the FTC's enforcement action against the social networking site Path (2013). Path was similar to, though smaller than, Facebook in that it let users create accounts, link to friends, upload pictures and text posts, share location information, and otherwise populate their profiles with information, including date of birth and gender. Path's legal problem was that it allowed users to create accounts even if their listed date of birth meant that their age was under thirteen. This meant that there were about 3,000 users for whom Path had actual knowledge that they were under thirteen (because Path knew their day and year of birth) and from whom Path collected extensive information. Path ultimately agreed to a $800,000 fine for this violation.[193]

[193] Federal Trade Commission, *Path Social Networking App Settles FTC Charges*, https://www.ftc.gov/news-events/news/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived-consumers-improperly-collected-personal.

F.T.C. and N.Y. v. Google LLC and YouTube, LLC (D.D.C. 2019)

Complaint

Congress enacted COPPA in 1998 to protect the safety and privacy of children online by prohibiting the unauthorized or unnecessary collection of children's personal information online by operators of Internet websites and online services. COPPA directed the Commission to promulgate a rule implementing COPPA. The Rule went into effect on April 21, 2000.

The Rule applies to any operator of a commercial website or online service directed to children under 13 years of age that collects, uses, and/or discloses personal information from children, or on whose behalf such information is collected or maintained. Personal information is "collected or maintained on behalf of an operator when . . . [t]he operator benefits by allowing another person to collect personal information directly from users of such Web site or online service." The definition of "personal information" includes, among other things, "first and last name," "online contact information," and a "persistent identifier that can be used to recognize a user over time and across different Web sites or online services," such as a "customer number held in a cookie . . . or unique device identifier."

The Rule can also apply to websites or online services that collect personal information from users of other child-directed websites or online services. Under the Rule, a website or online service is "deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another Web site or online service directed to children."

Among other things, the Rule requires a covered operator to give notice to parents and obtain their verifiable consent before collecting children's personal information online. This includes but is not limited to:

a) Posting a privacy policy on its website or online service providing clear, understandable, and complete notice of its information practices, including what information the website operator collects from children online, how it uses such information, its disclosure practices for such information, and other specific disclosures set forth in the Rule;
b) Providing clear, understandable, and complete notice of its information practices, including specific disclosures directly to parents; and
c) Obtaining verifiable parental consent prior to collecting, using, and/or disclosing personal information from children.

The Rule prohibits the collection of persistent identifiers for behavioral advertising absent notice and verifiable parental consent. Behavioral advertising, which also is referred to as personalized, targeted, or interest-based advertising, involves the tracking of a consumer's online activities in order to deliver tailored advertising based on the consumer's inferred interests.

Defendants provide a video-sharing platform on the Internet at www.youtube.com and on mobile applications (collectively, "YouTube") on which, among other things, consumers can view videos or upload video content to share.

In general, Defendants do not require users to register or create an account in order to view videos on YouTube. As a result, anyone can view most content on YouTube regardless of age. Defendants do limit certain activities on the platform, such as commenting on videos, to users that are logged in to a Google account.

In order to create a Google account, Defendants require the user to provide first and last name, e-mail address, and date of birth. A user can create an account by linking to an account "set up" page from any video or channel on YouTube, including videos and channels that are

directed to children. Defendants prevent users who identify as under 13 from creating an account.

In order to upload content on YouTube, users must have a Google account and then can create a "channel" to display their content. These users ("channel owners") can set "key words" for their channel that help other users searching for videos on YouTube find their channel. Channel owners can also set key words for individual videos they upload and choose whether to enable comments.

Eligible channel owners, which include commercial entities, can "monetize" their channel by allowing Defendants to serve advertisements to viewers, for which the channel owners and the Defendants earn revenue. Defendants enable behavioral advertising by default on monetized channels. When a channel owner monetizes a channel, Defendants collect information associated with a viewer's cookie or mobile advertising identifier in order to track the viewer's online activities and serve advertising that is specifically tailored to the viewer's inferred interests.

Beginning in January 2016, Defendants offered channel owners the option to disable behavioral advertising on their monetized channels. To turn off behavioral ads, the channel owners are required to actively check a box in the "Advertisements" section of YouTube's "Advanced Video Manager Options" menu. The checkbox that allows the channel owner to opt out of behavioral advertising contains text stating that doing so "may significantly reduce [the] channel's revenue." When a channel owner opts out of behavioral advertisements on a monetized channel, Defendants serve contextual advertising on the channel, which generates less revenue for the channel owner and Defendants.

YouTube and Kids

Defendants market YouTube to popular brands of children's products and services as a top destination for kids. For example, in a presentation to toy brand Mattel, maker of Barbie and Monster High, entitled "Insights on Families Online," Defendants stated, "YouTube is today's leader in reaching children age 6-11 against top TV channels." In a presentation provided to toy brand, Hasbro, maker of My Little Pony and Play-Doh, Defendants claimed that "YouTube was unanimously voted as the favorite website for kids 2-12," and that "93% of tweens visit YouTube to watch videos." In another presentation to Hasbro, Defendants referred to YouTube as "[t]he new 'Saturday Morning Cartoons.'" That presentation also claimed that YouTube was the "#1 website regularly visited by kids" and "the #1 source where children discover new toys + games."

Despite marketing YouTube as the "favorite website for kids 2-12," Defendants asserted on other occasions in email exchanges that channels on the platform did not need to comply with COPPA. For example, in response to one advertising company's questions regarding advertising on YouTube as it relates to a toy company and COPPA, Defendant Google's employee responded, "we don't have users that are below 13 on YouTube and platform/site is general audience, so there is no channel/content that is child-directed and no COPPA compliance is needed."

In addition to marketing YouTube as a top destination for kids, Defendants have a content rating system that categorizes content into age groups and includes categories for children under 13 years old. In order to align with content policies for advertising, Defendants rate all videos uploaded to YouTube, as well as the channels as a whole. Defendants assign each channel and video a rating of Y (generally intended for ages 0-7); G (intended for any age); PG (generally intended for ages 10+); Teen (generally intended for ages 13+); MA (generally intended for ages 16+); and X (generally intended for ages 18+). Defendants assign these ratings through both automated and manual review. Previously, Defendants also used a classification for certain videos shown on YouTube as "Made for Kids."

Defendants do not treat Y rated channels or videos differently for purposes of data collection from other content on YouTube. Defendants continue to allow the channel owner to monetize Y rated content and earn revenue from behavioral advertising. Defendants also had no policy in place to treat content classified as "Made for Kids" differently for purposes of behavioral advertising on YouTube.

In 2015, Defendants created a separate mobile application called "YouTube Kids," aimed at children age 2-12, generally using content rated Y or G taken from YouTube on an automated basis. Defendants also specifically curate, through manual review, content that appears on the YouTube Kids home screen, which Defendants refer to as the "home canvas." Content that appears on YouTube Kids continues to be available on YouTube. Unlike Defendants' practices on YouTube, Defendants do not collect persistent identifiers from users of YouTube Kids in order to serve behavioral advertising. Instead, Defendants monetize YouTube Kids solely through delivery of contextual advertising.

YouTube Hosts Numerous Child-Directed Channels

YouTube hosts numerous channels that are "directed to children" under the COPPA Rule. Pursuant to Section 312.2 of the COPPA Rule, the determination of whether a website or online service is directed to children depends on factors such as the subject matter, visual content, language, and use of animated characters or child-oriented activities and incentives. An assessment of these factors demonstrates that numerous channels on YouTube have content directed to children under the age of 13 . . . . Many of these channels self-identify as being for children as they specifically state, for example in the "About" section of their YouTube channel webpage or in communications with Defendants, that they are intended for children. In addition, many of the channels include other indicia of child-directed content, such as the use of animated characters and/or depictions of children playing with toys and engaging in other child-oriented activities.

Toy brand Mattel has several popular YouTube channels, including Barbie, Monster High, Hot Wheels, and Thomas & Friends. Content from each of these channels regularly appears on YouTube Kids and has been featured on its home canvas.

Cartoon Network is a popular YouTube channel that shows animated kids television shows, including Steven Universe, the Powerpuff Girls, and Teen Titans Go. The channel's content regularly appears on YouTube Kids and has been featured on its home canvas.

Hasbro's popular YouTube channel shows episodes of many animated kids programs, including My Little Pony, Littlest Pet Shop, Hanazuki, and Play-doh Town.

[Complaint continues to describe nine similar channels.]

Defendants earned close to $50 million from behavioral advertising on these channels, which represent only a few examples of the possible universe of child-directed content on YouTube.

Defendants Operate an Online Service Directed to Children

A website or online service is deemed directed to children where it has actual knowledge it is collecting personal information directly from users of another website or online service directed to children. 16 C.F.R. § 312.2. In numerous instances . . . Defendants have actual knowledge that they collect personal information, including persistent identifiers for use in behavioral advertising, from viewers of channels and content directed to children under 13 years of age. Defendants gained actual knowledge through, among other things, direct communications with channels owners, their work curating specific content for the YouTube Kids App, and their content ratings.

At no time did Defendants attempt to obtain verifiable parental consent from parents of viewers of these child-directed channels prior to the collection of personal information or provide parents with the COPPA-specified notice of their information practices.

Violations of the Children's Online Privacy Protection Rule

Defendants are "operators" as defined by the Rule. Defendants collect personal information from children under the age of 13 through YouTube channels that are websites or online services directed to children. Defendants have actual knowledge . . . that they collect personal information directly from users of these child-directed websites or online services. Therefore, under the COPPA Rule, Defendants are deemed to be operators of a child directed website or online service.

In numerous instances, in connection with the acts and practices described above, Defendants collected, used, and/or disclosed personal information from children in violation of the Rule, including by:

a) Failing to provide sufficient notice on their website or online service of the information they collect, or is collected on their behalf, online from children, how they use such information, their disclosure practices, and all other required content . . . ;
b) Failing to provide direct notice to parents of the information Defendants collect, or information collected on Defendants' behalf, online from children, how they use such information, their disclosure practices, and all other required content . . . ; and
c) Failing to obtain verifiable parental consent before any collection or use of personal information from children . . . .

Stipulated Order for Permanent Injunction and Civil Penalty Judgement, F.T.C. and N.Y. v. Google LLC and YouTube, LLC (D.D.C. 2019)

[Google and its subsidiary YouTube settled the charges. As part of the order, they paid $136 million to the FTC and $34 million to the state of New York. They also agreed to stop using the data collected previously from child-directed channels. Further:]

IT IS ORDERED that Defendants and Defendants' officers, agents, employees, and attorneys, and all other Persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with operating the YouTube Service, are permanently restrained and enjoined from:

(1) Failing to develop, implement, and maintain a system for Channel Owners to designate whether their Content on the YouTube Service is directed to Children. Such system shall include a Clear and Conspicuous notice that Content made available on the YouTube Service that is directed to Children may be subject to the Children's Online Privacy Protection Rule and that Channel Owners are obligated to designate such Content as directed to Children; and
(2) Failing to provide annual training regarding complying with the Children's Online Privacy Protection Rule for each Person responsible for managing Defendants' relationships with Channel Owners on the YouTube Service.
(3) Failing to make reasonable efforts, taking into account available technology, to ensure that a Parent of a Child receives direct notice of Defendants' practices with regard to the Collection, use, or Disclosure of Personal Information from Children, including notice of any material change in the Collection, use, or Disclosure practices to which the Parent has previously consented, unless the Children's Online Privacy Protection Rule provides an exception to providing such notice;

(4) Failing to post a prominent and clearly labeled link to an online notice of its information practices with regard to Children on the home or landing page or screen of its website or online service, and at each area of the website or online service where Personal Information is Collected from Children, unless the Children's Online Privacy Protection Rule provides an exception to providing such notice;
(5) Failing to Obtain Verifiable Parental Consent before any Collection, use, or Disclosure of Personal Information from Children, including consent to any material change in the Collection, use, or Disclosure practices to which the Parent has previously consented, unless the Children's Online Privacy Protection Rule provides an exception to Obtaining Verifiable Parental Consent; and
(6) Violating the Children's Online Privacy Protection Rule.

Statement of Chairman Joe Simons and Commissioner Christine Wilson

[The Commission split 3-2 on approving the settlement.]

First, [the settlement] requires Defendants to pay $136 million to the FTC and $34 million to New York. The $170 million total monetary judgment is almost 30 times higher than the largest civil penalty previously imposed under COPPA. This significant judgment will get the attention of platforms, content providers, and the public.

Second, the settlement includes strong conduct relief that goes beyond the technical requirements of COPPA. Indeed, as Commissioner Slaughter notes, this relief will change YouTube's business model going forward. Under COPPA, third parties that host and serve ads on child-directed content—but do not themselves create the content—are not responsible for making inquiries about whether the content is child-directed. This settlement now makes Defendants responsible for creating a system through which content creators must self-designate if they are child-directed. This obligation exceeds what any third party in the marketplace currently is required to do. It represents the first and only mandated requirement on a platform or third party to seek actual knowledge of whether content is child-directed.

Third, the complaint alleges two first impression applications of COPPA. First, the complaint alleges that individual channels on a general audience platform are "websites or online services" under COPPA. This framing puts content creators and channel owners on notice that we consider them to be standalone "operators" under COPPA, subject to strict liability for COPPA violations. Second, the complaint alleges that YouTube has liability under COPPA as a third party. When the Commission amended the COPPA Rule in 2013, we stated that platforms are not generally responsible for child-directed content that appears on them, unless the platform possesses actual knowledge that it is collecting personal information from users of a child-directed site or service. As detailed in the complaint, YouTube did possess actual knowledge as evidenced by its own marketing efforts, information received from channels, and its review of channel content to curate for the YouTube Kids App.

Dissenting Statement of Commissioner Rebecca Kelly Slaughter

To assess the effectiveness of the settlement's provisions, it is important to start with an understanding of YouTube's business model, which elucidates both why the alleged violations happened in the first place and whether they will be effectively curbed going forward. In sum and substance, YouTube partners with channel owners who, upon crossing a viewership threshold, can elect to monetize the channel to deliver advertisements to viewers; YouTube takes a 45% cut of the advertising revenue and passes the rest to the channel. Advertising on YouTube's channels can either be contextual (informed by the particular channel or video) or behavioral (informed by the behavior of the device owner as tracked across different websites, apps, and devices). YouTube has long allowed channel owners to turn off default behavioral advertising and serve instead contextual advertising that does not track viewers, but

vanishingly few content creators would elect to do so, in no small part because they receive warnings that disabling behavioral advertising can "significantly reduce your channel's revenue." In short, both YouTube and the channels have a strong financial incentive to use behavioral advertising.

Against this backdrop, I consider the proposed settlement. It is indisputable that the civil penalty negotiated here is historically large, but the injunctive relief is likely to have a more lasting impact. YouTube and Google have agreed to ensure that, every time a video is uploaded to YouTube by a content creator, the content creator will have to designate the video as child-directed or not. For videos designated as child-directed, YouTube will not serve behavioral advertisements or track persistent identifiers. This will help get a good portion of child-directed content out from under COPPA-violating behavioral advertising. Channels' designations of content as child-directed will give YouTube easily provable actual knowledge of the child directed nature of the content.

This relief is important, and I suspect it will result in a substantial amount of child directed content's being appropriately designated as such. While we cannot know for certain how creators will respond to the prompt to designate their content, I imagine that many high-profile content creators identified in the complaint—especially those such as Mattel and Hasbro who make most of their money from selling toys rather than from advertising—will forthrightly designate all of their child-directed content as child-directed. They will do so even though the contextual advertising served instead is far less lucrative because they will accurately predict that their risk of COPPA liability for deceitfully designating their content is high.

My concern is with the vast universe of content creators who will conduct a different cost-benefit analysis in which the perceived payoff of monetizing child-directed content through behavioral advertising outweighs the perceived risk of being caught violating COPPA. And that universe is indeed vast. Google marketed YouTube as the new "Saturday Morning Cartoons," but, unlike the Saturday morning cartoons of old, YouTube is not three channels—it is a virtually infinite smorgasbord of content with, according to recent estimates, more than 23 million channels that upload a combined 500 hours of video every minute. Many if not most of those channels are located outside the United States and therefore likely beyond COPPA's and the FTC's practical reach. Many are small enterprises with opaque operations that would be difficult subjects to investigate. Under the order, they will all have to make a designation of whether their content is child-directed. In light of the steep financial cost of such a designation—and the low likelihood of COPPA enforcement for channels under the radar or originating outside of the United States—it is reasonable to anticipate that there will be significant deceit.

And here is the heart of my objection: The order does not require YouTube to police the channels that deceive by mis-designating their content, such as by requiring YouTube to put in place a technological backstop to identify undesignated child-directed content and turn off behavioral advertising. True, a technological backstop is not explicitly mandated by COPPA's text, but such a requirement would, I believe, be appropriate and necessary fencing-in relief. The order's requirement that channel owners designate content as child-directed is also not required by COPPA, yet it is a good start to fencing-in relief, to which YouTube has consented, to redress YouTube's own COPPA violations and reduce its facilitation of others' violations. Fencing-in relief that goes beyond bare-minimum statutory requirements is a common and important aspect of effective Commission orders.

Dissenting Statement of Commissioner Rohit Chopra

Despite this authority to ensure that bad actors are meaningfully penalized for violating children's privacy, the Commission is agreeing to a settlement that will result in Google profiting from its violations.

Some of my colleagues assert that the "penalty" exceeds Google's gains. I respectfully disagree. As part of the evidence I evaluated in this investigation, I reviewed the revenues generated from behavioral advertising on [redacted], which totaled [redacted] million during the period from [redacted]. If we use this data across [redacted] and extend this time period to the full period of noncompliance, while also factoring in a revenue growth rate of [redacted], we yield ill-gotten gains in excess of [redacted] million.

This estimate may even be conservative, as it does not consider Google's avoided costs of compliance, any ill-gotten gains from data being used by Google's other properties, the increased value of its predictive algorithm trained by ill-gotten data (which will not be reversed), and other considerable benefits from lawbreaking. Using this conservative base of ill-gotten gains, I favor using a calibrated multiplier for penalties to reflect clear congressional intent to penalize wrongdoers. For example, in the Commission's 2012 action against Google, the FTC obtained a penalty of more than five times the company's unjust gains. Had we used a similar multiplier, that would result in a target of [redacted] billion.

[…]

First, Google's privacy practices are highly problematic, and I thank the staff from the New York Attorney General and the FTC for investigating it. However, I agree with Commissioner Slaughter's assessment of the injunctive provisions of the settlement. They are insufficient, and I would add that Google and YouTube made a business decision to allow behavioral advertising without human review. The settlement's provisions requiring a function for content creators to disclose whether the content is child-directed may have the perverse effect of allowing Google to pin the blame on content creators, even when they already know when YouTube videos are clearly for children. Absent an enforceable commitment from Google that it will fundamentally change its business practices to ensure that child-directed content is not subject to impermissible data harvesting, children will still be at risk.

Second, in my view the Commission often makes a low opening bid for monetary relief. Then, Commissioners point to litigation risk, lack of clear authority, and resource constraints to rationalize an outcome that allows a defendant to profit from the wrongdoing. Financial penalties need to be meaningful or they will not deter misconduct.

If Congress enacts privacy legislation, it should not cut and paste COPPA's approach to penalties. It should move away from vague factors for civil penalties and shift toward ones that are easier for agencies and courts to administer. There are many alternative approaches, such as requiring a minimum penalty per violation, adjusted upward if the violation is intentional or reckless. In addition, Congress should give *all* enforcers of any privacy law a robust set of enforcement tools, including penalties. In COPPA, state attorneys general can only seek forfeiture of ill-gotten gains and refunds to victims, but not financial penalties beyond that. In this matter, the New York Attorney General was unable to pursue civil penalties, since the FTC has exclusive authority to do so. This should change.

Notes

1. As with the Facebook case above, here we see a fine that is both the largest ever assigned for a particular form of misconduct as well as potentially far too low. What was it worth to YouTube to be sloppy on COPPA compliance for years? If you had told YouTube executives that they would ultimately be fined 170 million for their misconduct, would they have pushed ahead anyway? Quite possibly yes; time and time again we have seen companies choose to pursue increased short-term profits despite regulatory risk.
2. Speaking of risk, there is also some litigation risk here for the FTC. This is a rare case imposing third-party COPPA liability. Recall the language from 16 C.F.R. § 312.2: "A website or online service is deemed directed to children where it has actual knowledge it is collecting personal information directly from users of another website or online service

directed to children." How well does this fit what YouTube was doing in this case? Were there any good arguments for the defense to make?

3. How valuable is the self-certification required by the order? Does requiring channels to self-identify as child-directed solve a huge portion of the problem (reputable actors will follow the rules, as even Slaughter's dissent acknowledges), or is it weak tea, allowing many less-established actors to lie?
4. Slaughter's dissent pushes an interesting argument. Though COPPA does not require the automatic detection of child-directed content, YouTube is perfectly capable of creating programming that does so. Is she right that YouTube should have been required to do so? If so, should all companies be held to that standard? Requiring companies to have that kind of AI/machine learning tool would seriously impact young startups. But YouTube itself is already well on the path to having such tools, with its content rating and ad-targeting systems.

United States v. Epic Games, Inc. (E.D.N.C. 2022)

Complaint for Permanent Injunction, Civil Penalties, and Other Relief

Epic Games, Inc. ("Epic," "Epic Games," or "Defendant") is the developer and distributor of the hit online video game "Fortnite." Through Fortnite, Epic matches children and teens with strangers around the world in interactive gameplay, encourages real-time communications by featuring on-by-default voice and text chat features, and publicly broadcasts players' account names. Even though Fortnite is directed to children, and even when Epic had actual knowledge that Fortnite users were children, Epic failed to comply with the COPPA Rule's parental notice, consent, review, and deletion requirements. Although Epic has changed its practices over time, those changes have not cured the violations.

Ultimately, Epic's matchmaking children and teens with strangers while broadcasting players' account names and imposing live on-by-default voice and text communications has caused substantial injury that is neither offset by countervailing benefits nor reasonably avoidable by consumers. Children and teens have been bullied, threatened, and harassed within Fortnite, including sexually. Children and teens have also been exposed to dangerous and psychologically traumatizing issues, such as suicide and self-harm, through Fortnite. And the few relevant privacy and parental controls Epic has introduced over time have not meaningfully alleviated these harms or empowered players to avoid them.

Children's Online Privacy Protection Rule

Congress enacted COPPA in 1998 to protect the safety and privacy of children online by prohibiting the unauthorized or unnecessary collection of children's personal information online by operators of Internet websites and online services. COPPA directed the Commission to promulgate a rule implementing COPPA. The Commission promulgated the COPPA Rule on November 3, 1999 . . . .

The Rule applies to any operator of a commercial website or online service directed to children under 13 years of age that collects, uses, and/or discloses personal information from children, and to any operator of a commercial website or online service that has actual knowledge that it collects, uses, and/or discloses personal information from children. The Rule requires an operator to meet specific requirements prior to collecting, using, or disclosing children's personal information online, including but not limited to:

a) Posting a privacy policy on its website or online service providing clear, understandable, and complete notice of its information practices, including what information the operator collects from children online, how it uses such information, its disclosure practices for such information, and other specific disclosures set forth in the Rule;

b) Providing clear, understandable, and complete notice of its information practices, including specific disclosures, directly to parents;
c) Obtaining verifiable parental consent prior to collecting, using, and/or disclosing personal information from children;
d) Providing a reasonable means for parents to review personal information collected from children online, at a parent's request; and
e) Deleting personal information collected from children online, at a parent's request.

Epic is the developer of Fortnite, a hit online video game available to players on multiple consoles. Launched in July 2017, Fortnite quickly caught the attention of young consumers—teens and children under age 13—in the United States and abroad and, today, has more than 400 million players.

Available in different modes, Fortnite is generally free to download and play (although one mode, called "Save the World," costs money). Epic has earned billions of dollars in revenue through Fortnite, primarily by selling Fortnite players in- game digital content like costumes (called "cosmetics" or "skins") and dance moves (called "emotes") for their avatars, and through licensing partnerships with companies selling Fortnite-branded merchandise.

To play Fortnite using a personal computer or mobile device, players must first create an Epic Games account. Prior to September 2019, anyone could create an Epic Games account by providing Epic Games with their first name, last name, and email address, and choosing a name (called a "display name") for their account. This remains the process for players located outside the United States and Europe. For players in the United States or Europe, however, Epic began requiring birthdate information as part of the account creation process on September 11, 2019 (for U.S. players), September 2, 2021 (for U.K. players), and November 30, 2021 (for European players outside the U.K.).

Regardless of the console or type of account a player uses, several social features are enabled within Fortnite by default that convert the game into a platform for connecting with other players. Among other things, these social features allow players to find and friend each other (by display name), play matches together, exchange personal information, and converse with each other in real time by voice and text. On the backend, Epic collects and uses various unique device IDs, account IDs, and other persistent identifiers to keep track of players' progress, purchases, settings, and friends lists, among other player-specific information.

Fortnite Is Directed to Children Under 13

Considering the factors set forth in the COPPA Rule, including the game's subject matter, use of animation, child-oriented activities and language, and music content, evidence of intended audience, and empirical evidence about the game's player demographics, Fortnite is directed to children under age 13.

Fortnite's Gameplay, Visual Content, and Features are Directed to Children

Revolving around a "shooter-survival" style of gameplay, Fortnite's various game modes include "build-and-create" mechanics like those in other games popular with children, and feature other elements that appeal to children, like cartoony graphics and colorful animation. For example, in Fortnite's popular "Battle Royale" mode, players' colorful avatars enter the game by hang gliding to various places in a virtual world (e.g., "Loot Lake," "Tilted Towers," "Retail Row") after jumping from a whimsical flying blue school bus, called the "Battle Bus." Akin to digital laser tag, there is no blood or gore in Fortnite, and players are "eliminated" from the game (not "killed").

Prominent in Fortnite gameplay is an emphasis on building "forts" and other creations—offering children a digital playground to explore. As Epic noted when announcing the game's release in 2017, the "soul of Fortnite" derives from the common childhood experience of fort-

building—"whether it was blankets and couch cushions, or building a fort in the woods by your house, you and your friends could spend Saturday afternoons hiding out, or repelling hordes of imaginary creatures"—and the game incorporates "sculpted 'puzzle pieces' to create interesting play spaces to explore."

Fortnite Theming Decisions Ensure Content Appeals to Children

Epic strives to create a "Living room safe, but barely" environment using content that appeals to children when making Fortnite theming decisions, including potential music, celebrity, and brand partnerships. In so doing, Epic Games employees have explained:

"We want to be living room safe, but barely. We don't want your mom to love the game – just accept it compared to alternatives"

"Agree with the idea that, generally, all theming should be relevant to a 8-14 y.o., as a litmus test"

"We are NOT adult: experience must allow for parental comfort for ages 10+"

Based on these guiding principles, Fortnite has promoted and hosted live in-game concerts featuring celebrities popular with children, such as Marshmello, Travis Scott, Ariana Grande, and BTS.

Epic Has Made Millions in Royalties Selling Official Fortnite Toys, Halloween Costumes, and Youth Apparel

Further evidencing the game's intended audience, Epic has made millions in royalties by partnering with companies to sell officially licensed Fortnite merchandise for children. Within a year of Fortnite's public release, Epic retained a licensing agent and launched a consumer products program to give players official Fortnite-branded merchandise.

Acknowledging that "Youth and Kids are obsessed with Fortnite" and "want to show their allegiance to their favorite pastime," Epic's agent developed a licensing plan with a "core" component that targeted "Kids" and "Youth Universes," and worked closely with Epic to broker partnerships between Epic and other companies to create Fortnite-branded costumes, toys, books, youth-sized apparel, and "back to school" merchandise . . . .

In its first consumer products deal, Epic partnered with Spirit Halloween to offer officially licensed Fortnite Halloween costumes. Available in children's sizes, these costumes have been very popular with kids . . . . Indeed, Spirit Halloween sold hundreds of thousands of child-sized Fortnite costumes between 2018 and 2020, which account for more than half of all Fortnite costumes sold by Spirit Halloween during those years.

[Complaint reviews several similar toy licensing deals, including child-direct television advertising.]

Many Children Play Fortnite, and Many Fortnite Players Are Children

Not surprisingly, empirical evidence shows that many children play Fortnite, which is disproportionately popular with "tweens." For example, publicly available survey results from a 2019 report show that 53% of U.S. children aged 10-12 played Fortnite weekly, compared to 33% of U.S. teens aged 13-17, and 19% of the U.S. population aged 18-24._bookmark0 And Epic, which had previously contracted with the company that conducted this survey (to conduct a different survey in connection with Fortnite), received pre-publication copies of the survey results along with a private briefing by the researchers who conducted the survey.

Results from Epic's own player surveys are consistent with this data. The results show that most Fortnite players (i.e., approximately 70%) live at home with their parents or guardians, and, of those who live with their parents or guardians, most (i.e., approximately 80%) identify as students.

Fortnite's Unfair Default Settings Have Harmed Children and Teens

Predictably, Epic has caused substantial harm by matching children and teens with strangers in interactive gameplay while publicly broadcasting players' display names and imposing real-time communications through on-by-default voice and text chat.

Epic has known about this harm and nevertheless allowed it to persist. Shortly after Fortnite's launch, Epic's then Director of User Experience ("UX") emailed Epic leadership in August 2017 seeking "basic toxicity prevention" mechanisms—noting that "surely a lot of kids" were currently playing the game, and imploring Epic to "avoid voice chat or have it opt-in at the very least." To no avail. Voice chat remained on by default . . . . While Epic contemporaneously added a toggle on a settings page enabling those who happened to find it to switch voice chat off, the feature remained on as part of Fortnite's default configuration for all players.

Within two weeks of Epic's October 2017 decision to enable voice chat in Battle Royale, a high-profile gamer verbally harassed a young player while publicly streaming to an audience of thousands of viewers. As an Epic Games employee acknowledged: "[W]e honestly should have seen this coming or [at least] expected this with an on-by-default voice chat system. Situations like this are bound to happen . . . ." But Epic again declined to modify its on-by-default voice chat system (or implement any other changes) to stop subjecting kids to such abuse within Fortnite.

Eight months later, in June 2018, Epic's UX research team analyzed the parental and privacy controls offered by a wide range of other games and game platforms, and presented the results of their assessment to Epic executives and other employees. Epic's UX team reiterated their recommendation to move to an opt-in voice chat configuration for Fortnite, noting that most players did not use the feature when playing with strangers, which presented "a risk in terms of negative social behavior," and acknowledging "[f]rom social/media stories we have seen both 'Fortnite is positive' and 'child charity warns parents about predators in Fortnite.'" Epic leadership praised the "very well-researched and thoughtful" work, but the UX team "got no traction" around opt-in voice chat. Epic continued to reject the UX team's recommendation.

All the while, kids have been bullied, threatened, and harassed, including sexually, through Fortnite. Numerous news stories chronicle reports of predators blackmailing, extorting, or coercing children and teens they met through Fortnite into sharing explicit images or meeting offline for sexual activity.

In addition, Epic's Fortnite practices have exposed kids to dangerous and psychologically traumatizing issues, such as suicide and self-harm.

As reflected in internal exchanges between Epic employees, these harms are not outweighed by countervailing benefits, nor are they reasonably avoidable by consumers. Shortly before the UX team's unsuccessful push to convince leadership to change Fortnite's default settings in June 2018, an Epic employee who had helped create Fortnite emailed Epic's PR manager and Epic's Creative Director:

> I think you both know this, but our voice and chat controls are total crap as far as kids and parents go. It's not a good thing. It was on my list a year ago, but never bubbled to the surface. This is one of those things that the company generally has weak will to pursue, but really impacts our overall system and perception. I've made a coppa [sic] compliant game and we are far from it, but we don't need to be that far . . .

To which Epic's PR manager responded:

> 100% agree here. Communication-wise, we are staying out of the debate, even though Fortnite is right in the middle of it. We'd come out looking way better if

> we offered the proper tools across the board here. I agree the best response is doing the right thing, and not debating it . . .

The employee then forwarded the exchange to Epic's lead UX researcher, who replied "I would really like to see even the small step of on first load asking if people want voice on or off. Even hardcore games like Monster Hunter have done this." And when articulating the UX team's position to Epic executives a week later, Epic's lead UX researcher noted a good opt-in system yielded only upside: it would align with players' reported preferences, preserve the feature's utility, and reduce toxicity ("[f]or example when Riot moved to opt-in text chat they saw the same volume of chat usage, but reduced toxicity as those who want to chat were able to communicate and those that did not were not exposed").

Epic did introduce a toggle switch allowing Fortnite players to turn voice chat off, but the control was buried on a hard-to-find settings page. As one Fortnite programmer lamented:

> So when I was at my brothers house, and was watching my 10 yr old nephew play. I'm like, hey, why is there no sound on the TV? And he's like, we turn off the volume because you can hear people talking. People related to me by blood were no sh[**] muting the TV instead of looking for a way to disable voice chat. Not a proud day . . . The settings are not a land most folks venture to, certainly not technophobic parents . . .

When this message was forwarded to Epic's lead UX researcher, he responded with exasperation: "Sigh. Can we just suggest popping up a dialog asking people if they want it on or not?"

Epic's Changes Have Not Cured the Law Violations

Over time, Epic has introduced a few changes to Fortnite in weak-willed attempts to provide players and their parents with some privacy and parental controls, and comply with COPPA's parental notice, consent, review, and deletion requirements. But these overdue efforts have not cured the law violations.

Epic Has Consistently Resisted, Deprioritized, and Delayed Privacy and Parental Controls

Fortnite launched with no parental controls and minimal privacy settings. Initially, the only such options consisted of a few settings allowing players to "mute," "block," or "kick" (i.e., remove from shared gameplay activities) individual problematic players they encountered, or narrow the set of players who could join them in collaborative gameplay (i.e., by changing their "Party Privacy" setting from "public" to "friends of friends," "friends," or "private"). Neither players nor their parents could prevent a player's display name from being publicly broadcast or disable voice and text chat (except by using parental controls and voice chat settings when playing Fortnite on gaming consoles that provide such controls and settings).

Shortly after launch, Epic introduced the toggle switch discussed above, allowing Fortnite players to disable voice chat, but did not inform players of the setting's availability and placed the control in the middle of a detailed settings page.

In June 2019, nearly two years after Fortnite's launch, Epic finally introduced parental controls to the game. Starting on that date, parents could set a PIN code that must be entered to adjust various privacy settings—i.e., Auto Decline Friend Requests, Hide Other Player Names, Anonymous Mode, and Voice Chat. Of course, to enable parental controls, parents would first need to know they existed, have access to their child's or teen's Fortnite account, and know where to find the controls.

For More Than Two Years, Epic Took No Steps to Seek Parental Consent Before Collecting Children's Personal Information or Explain How the Company Handled It

From July 2017, when Fortnite launched, until September 2019, Epic took no steps to (a) provide a direct notice to parents describing Epic's practices regarding the collection, use, and disclosure of children's personal information; (b) explain what information Epic collected from children through Fortnite; or (c) seek verifiable parental consent ("VPC") from parents before collecting their children's personal information through Fortnite.

Instead, Epic included one paragraph on the second-to-last page of its global privacy policy disavowing that it directed any services to children or intentionally collected any personal information from such players, and asking parents to contact Epic if they believed Epic had received personal information from their child:

> Epic does not direct its websites, games, game engines, or applications to children (usually considered to be under the age of 13, depending on the country where you reside). We also do not intentionally collect personal information from children through our websites, games, game engines, or applications. If you are the parent or guardian of a child and you believe that we have inadvertently received personal information about that child, please contact us as described in the How to Contact Us section of this policy and we will delete the information from our records.

When parents contacted Epic to review or delete the information Epic collected from their child through Fortnite, or delete their child's Epic Games account, and those parents did not have access to their child's Fortnite account, Epic made those parents jump through extraordinary hoops to "verify" their parental status. For example, Epic required some parents to provide all IP addresses used by their child to play Fortnite, the date the child's Epic Games account was created, an invoice ID for an Epic Games purchase . . . [several additional requirements omitted]. Where parents were able to provide such information, Epic sometimes required them to provide *even more* information before Epic would agree to process the parent's review or deletion request—like the name of a cosmetic item their child purchased more than 30 days ago *and* a copy of the parent's passport, identification card, or recent rent or mortgage statement.

Even when Epic obtained actual knowledge that particular Fortnite players were under 13, Epic took no steps to comply with COPPA. Indeed, Epic went to great lengths to pretend it never obtained actual knowledge at all.

In March 2018, Microsoft personnel told Epic that Epic would have to block Xbox accounts belonging to children under 13 from participating in cross-console gameplay through Fortnite. In particular, Microsoft wanted Epic to use an existing Xbox mechanism (an API called the UserAgeGroup) to check whether a given Xbox player was using an "Adult," "Child," "Teen," or "Unknown" Xbox account, and block any Xbox players using "Child" accounts (defined as accounts belonging to players under age 13) from using Fortnite's cross-console gameplay feature. In other words, Microsoft wanted Epic to use Microsoft's API to determine which Xbox accounts belonged to children under age 13 and block those accounts from participating in Fortnite's cross-console gameplay feature.

Although Epic initially resisted, the company ultimately acquiesced and began blocking Xbox accounts identified via the UserAgeGroup API as belonging to a player under 13 from participating in cross-console gameplay within Fortnite. But Epic did not take any other steps to limit those players' communications with third parties, seek VPC for them, provide their parents with any notices explaining how Epic handled children's personal information, or otherwise comply with COPPA. Instead, as reflected in company records, Epic pretended they had no idea these players were children for any purpose other than determining whether they could participate in cross-console gameplay.

Epic's Dilatory COPPA Measures Fail to Comply With The Law

Epic eventually began to change its approach to COPPA compliance. On September 11, 2019 . . . Epic introduced an age gate to the account creation process for prospective Fortnite players attempting to create an Epic Games account on the Epic Games website from an internet connection with a U.S. IP address. For any such prospective player who self-identified as being 12 years old or younger, Epic would collect a parent's email address from the player and send an email to the player's parent describing how Epic handled children's personal information and asking the parent to complete a VPC process—such as using a credit card to make a small refundable charge.

But this initiative had no effect on the default configurations of Fortnite players' privacy controls—which continue to enable the public broadcast of players' display names and direct communication between players, regardless of a player's age.

Nor did Epic's September 11, 2019, changes apply to the hundreds of millions of Fortnite players who already had accounts, with a few limited exceptions. In the weeks before implementation, Epic employees searched Fortnite player support tickets to find those with indicia that a U.S. player may be under the age of 13. These efforts surfaced 36,000 such tickets, which Epic associated with 15,300 identifiable Fortnite players. Regardless of whether a ticket specifically identified a particular player as being under 13, or merely suggested that a player might be under 13, Epic logged all 15,300 players out of their accounts and asked them to provide their birthdate the next time the player attempted to log in—emailing parents a direct notice and asking them to complete a VPC process only if the player then self-identified as being under age 13.

Around the same time, Epic began changing how it handled emails identifying specific Fortnite players as being age 12 or younger. Previously, Epic did not take any steps to ensure the company sought VPC for such players or provided such players' parents with any notices describing how Epic handled their children's personal information. But starting in late 2019, Epic began forwarding these types of emails to player support agents, who try to determine whether the underlying player is based in the U.S. If so, and if the player has not already been subjected to Epic's age gate, the player is logged out and required to provide their birthdate the next time the player attempts to log in. Only if the player then self-identifies as being twelve or younger does Epic send their parent a direct notice and seek VPC.

Based on the facts and violations of law alleged in this Complaint, the FTC has reason to believe that Defendant is violating or is about to violate laws enforced by the Commission.

Count I - COPPA Rule

In numerous instances, in connection with the acts and practices described above, Defendant collected, used, and disclosed personal information from children younger than age 13 in violation of the Rule by:

a) Failing to provide notice on its website or online service of the information it collects online from children, how it uses such information, and its disclosure practices, among other required content, in violation of Section 312.4(d) of the Rule, 16 C.F.R. § 312.4(d);
b) Failing to provide direct notice to parents of the information it collects online from children, how it uses such information, and its disclosure practices for such information, among other required content, in violation of Section 312.4(b) of the Rule, 16 C.F.R. § 312.4(b);
c) Failing to obtain consent from parents before any collection or use of personal information from children, in violation of Section 312.5(a)(1) of the Rule, 16 C.F.R. § 312.5(a)(1);
d) Failing to provide, at the request of parents, a means of reviewing any personal information collected from children, in violation of Section 312.6(a)(3) of the Rule, 16 C.F.R. § 312.6(a)(3); and
e) Failing to delete, at the request of parents, personal information collected from children, in violation of Section 312.6(a)(2) of the Rule, 16 C.F.R. § 312.6(a)(2).

Count II - Unfair Default Settings

Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

As described . . . above, Defendant has developed and operated, and continues to develop and operate, a ubiquitous, freely-available, and internet-enabled video game directed at children and teens that publicly broadcasts players' display names while putting children and teens in direct, real-time contact with others through on-by-default lines of voice and text communication. Even after instituting an age gate on its service, Defendant has continued to broadcast display names and enable such direct communication by default for all players, including children who identify themselves as under 13 and young teens.

As described . . . above, Defendant's actions cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

Notes

1. Online games want to be able to treat their users as adults because adults can freely interact with each other, independently spend money, and are largely responsible for their own drama. Children, on the other hand, need some amount of protection and some amount of permission to spend money. So Epic Games would really prefer if its users were adults or, at least, could be treated as adults. But that was simply not their user base and they knew it.
2. Following the FTC complaint, Epic Games reached a 520-million-dollar settlement in 2022, 275 million for COPPA violations and 245 million for tricking users into unwanted transactions.[194] Beyond the monetary fine, the settlement required Epic Games to disable voice and text chat unless it obtains parental consent for children under 13 or user consent for teenagers. Epic was also required to delete all data collected in violation of COPPA, establish a comprehensive privacy program, and submit to independent privacy audits. Additionally, Fortnite has rolled out "cabined accounts" with heightened privacy settings for underage players awaiting parental consent and implemented parental control over friend requests, in-game purchases, and daily spending limits.[195]
3. Note here that Epic Games is also being pursued under a Section 5 unfair practices claim. Much of what Epic Games was doing was sketchy, but not actually relevant under COPPA. But having caught the FTC's attention, it was not going to address only some of the issues that were raised. Also, to what extent should the FTC distinguish between adult-directed and child-directed products under Section 5? Is it proper for the agency to say that a default setting is particularly unfair because it is being applied to children? When, and when not?

2) California Age-Appropriate Design Code Act

State legislatures have passed a flood of laws aimed to protect children online. Support for various flavors of these laws has come from across the political spectrum, yet serious policy and constitutional concerns are raised by them. Consider as an example this litigation over California's recently passed law.

---

[194] Press Release, Fed. Trade Comm'n, *Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges* (Dec. 19, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations.

[195] Epic Games, *Epic FTC Settlement and Moving Beyond Long-Standing Industry Practices* (Dec. 19, 2022), https://www.epicgames.com/site/en-US/news/epic-ftc-settlement-and-moving-beyond-long-standing-industry-practices.

NetChoice, LLC v. Bonta, 170 F.4th 744 (9th Cir. 2026)

M. SMITH, Circuit Judge:

In 2022, the California legislature unanimously enacted the CAADCA, Cal. Civ. Code §§ 1798.99.28–1798.99.40. The Act's stated purpose is to protect the "privacy, safety, and well-being of children" when engaging with online products and services that "children are likely to access." To that end, the CAADCA applies only to those businesses that provide "an online service, product, or feature likely to be accessed by children" under the age of eighteen. An online service is "likely to be accessed by children" when "it is reasonable to expect, based on [enumerated] indicators, that the online service, product, or feature would be accessed by children."

In service of its goals concerning children's data privacy, the CAADCA imposes certain affirmative obligations and prohibitions on the businesses it regulates. For example, in 2024, this same panel of our court affirmed a preliminary injunction as to the provision requiring covered online businesses to create a Data Protection Impact Assessment (DPIA) report, or a "systematic survey to assess and mitigate risks that arise from the data management practices of the business to children who are reasonably likely to access the online service ... that arises from the provision of that online service[.]" *See NetChoice, LLC v. Bonta* (*NetChoice I*), 113 F.4th 1101, 1116–22 (9th Cir. 2024). That requirement remains enjoined and is not at issue in this appeal.

This appeal concerns the CAADCA's coverage definition, Cal. Civ. Code § 1798.99.30(b)(4)(A)–(F); age estimation requirement, *id.* § 1798.99.31(a)(5); and data use and dark patterns restrictions, *id.* §§ 1798.99.31(b)(1)–(4), (7). The California Attorney General has authority to enforce the CAADCA. Violators face civil penalties of up to $2,500 per child for each negligent violation and up to $7,500 for each intentional violation.

The Act previously included a safe-harbor provision that allowed noncompliant businesses to cure an alleged violation within 90 days of written notice from the Attorney General of the alleged violation. We affirmed a preliminary injunction enjoining that notice-and-cure provision in *NetChoice I*, 113 F.4th at 1125.

FACTUAL & PROCEDURAL BACKGROUND

NetChoice is trade association whose members consist of large technology companies like Amazon, Google, Meta, and Netflix. In 2022, before the CAADCA took effect, NetChoice brought suit challenging the Act on constitutional and federal preemption grounds. It also moved for a preliminary injunction. The district court granted that motion and enjoined the CAADCA in full, concluding that NetChoice was likely to succeed on the merits of at least one of its facial theories under the First Amendment. *NetChoice, LLC v. Bonta*, 692 F. Supp. 3d 924, 965–66 (N.D. Cal. 2023).

The State appealed. While that appeal was pending, the United States Supreme Court decided *Moody v. NetChoice, LLC*, 603 U.S. 707 (2024), where it clarified the standard for a facial challenge under the First Amendment. We applied the *Moody* standard in *NetChoice I* and determined that the district court did not conduct the proper analysis for a First Amendment facial challenge. We therefore vacated the majority of the preliminary injunction and remanded to the district court for further proceedings. However, we affirmed the preliminary injunction with respect to the DPIA requirement, concluding that it likely facially violates the First Amendment. We likewise affirmed the district court's decision to enjoin the enforcement of other provisions not grammatically severable from that requirement.

On remand, NetChoice filed a first amended complaint (FAC) and a second motion for a preliminary injunction. The FAC asserted a new facial First Amendment challenge to the CAADCA: that the Act's coverage provision, making the Act applicable to online businesses that

are "likely to be accessed by children," is content based and fails strict scrutiny, thus rendering the CAADCA's substantive provisions unconstitutional in every application. The FAC also asserted as-applied challenges to the CAADCA. NetChoice's second preliminary injunction motion advanced these newly pleaded theories as additional grounds for enjoining the CAADCA's enforcement.

Ruling on that motion, the district court agreed with NetChoice that the coverage provision defining "likely to be accessed by children" is content based and triggers First Amendment scrutiny for the entire statute. The district court then held that the CAADCA likely fails strict scrutiny because it "applies to *all* online content likely to be accessed by consumers under the age of 18, and imposes significant burdens on the providers of that content," and the State had failed to show that the CAADCA is narrowly tailored, in part because its "interest in protecting the privacy and well-being of children" could be advanced "by vigorous enforcement of existing, less restrictive regulations."

Because, as the district court noted, some courts have construed *Moody* to require analyzing facial challenges provision-by-provision, the district court also addressed NetChoice's challenges to individual provisions of the CAADCA. It first concluded that all the CAADCA's "[p]rovisions are subject to strict scrutiny because of the content-based coverage definition." The district court then determined that NetChoice was not likely to succeed on its facial First Amendment challenge to the data use restrictions or the dark patterns restriction but that NetChoice was likely to succeed on its First Amendment challenge to the age estimation requirement. However, the district court concluded that NetChoice was likely to succeed on its vagueness challenges to the data use restrictions and dark patterns restriction but not to the age estimation requirement. NetChoice also challenged, and the district court enjoined, the CAADCA's policy enforcement requirement, Cal. Civ. Code § 1798.99.31(a)(9). Next, the district court turned to severability and held that no part of the CAADCA was volitionally separable from the enjoined notice-and-cure provision.

The district court then addressed NetChoice's claims that the CAADCA is preempted by Section 230 of the Communications Decency Act (Section 230), 47 U.S.C. § 230(c), preempted by the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–06, and facially invalid under the Dormant Commerce Clause. In part because the parties dedicated insufficient briefing on these issues, and based on the record before it, the district court concluded that NetChoice was not likely to succeed on the merits of any of these claims. Similarly, because NetChoice had "devote[d] a single sentence of its [preliminary injunction] motion to its as-applied claims" and did not address the factors required for an as-applied challenge, the district court denied NetChoice's motion on that ground.

Because the district court concluded that NetChoice met the remaining preliminary injunction factors on its facial claim as to the coverage definition, on severability grounds, and on some of its challenges to the Act's individual provisions, the district court granted NetChoice's motion for a preliminary injunction and enjoined the CAADCA in its entirety. The State timely appealed.

ANALYSIS

To obtain a preliminary injunction, NetChoice must show that (1) it is likely to succeed on the merits; (2) it is likely to suffer irreparable harm in the absence of preliminary relief; (3) the balance of equities tips in its favor; and (4) an injunction is in the public interest. The party seeking a preliminary injunction bears the burden of proving each element. As in its last round before our panel, the State does not meaningfully contest the latter three preliminary injunction factors. We therefore focus our analysis on whether NetChoice is likely to succeed on the merits of its facial challenges to the CAADCA as a whole and to its individual provisions.

I. NetChoice is not likely to succeed on the merits of its facial challenge to the CAADCA's coverage definition.

Under the First Amendment, "[c]ontent-based laws—those that target speech based on its communicative content—are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015). In turn, "[g]overnment regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed." Courts may determine whether a regulation is content based by considering whether it "draws distinctions based on the message a speaker conveys" "on its face." Even "subtle ... distinctions" that "defin[e] regulated speech by its function or purpose" are "subject to strict scrutiny."

The Supreme Court has also recognized "a separate and additional category of laws that, though facially content neutral, will be considered content-based regulations of speech: laws that cannot be justified without reference to the content of the regulated speech." "Those laws, like those that are content based on their face, must also satisfy strict scrutiny." *Id.*; *see also Sorrell*, 564 U.S. at 566 ("Even if the hypothetical measure on its face appeared neutral as to content and speaker, its purpose to suppress speech and its unjustified burdens on expression would render it unconstitutional.").

Our First Amendment analysis proceeds in three steps. "The first step ... is to determine whether the regulation implicates protected expression." Thus, "[t]he threshold question is whether conduct with a 'significant expressive element' drew the legal remedy or the [statute] has the inevitable effect of 'singling out those engaged in expressive activity.' " Next, we ask "whether the [statute] is content based or content neutral." If the statute is content based, we must determine whether it withstands strict scrutiny. If it is content neutral, the statute need only satisfy intermediate scrutiny.

But that is not all: NetChoice must also satisfy the requirements for a facial challenge as to each challenged provision. In *Moody*, the Supreme Court explained that district courts evaluating a facial challenge under the First Amendment must assess "whether a substantial number of [the law's] applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." That analysis proceeds in two steps of its own. First, courts must "assess the state law['s] scope" by asking "[w]hat activities, by what actors, do the laws prohibit or otherwise regulate?" Second, courts must "decide which of the law['s] applications violate the First Amendment, and ... measure them against the rest." A facial challenge thus "demands record development on third-party speech and the full scope of a law's potential applications." Here, "[i]t is NetChoice's burden to make those showings."

A. NetChoice does not carry its burden for its facial challenge to the coverage definition under *Moody*.

The CAADCA applies to any "business that provides an online service, product, or feature likely to be accessed by children." Cal. Civ. Code § 1798.99.31(a). The Act defines "likely to be accessed by children" to mean that "it is reasonable to expect, based on [enumerated] indicators, that the online service, product, or feature would be accessed by children." *Id.* § 1798.99.30(b)(4). The definition relies on application of the following indicators:

A. The online service, product, or feature is directed to children as defined by the Children's Online Privacy Protection Act (15 U.S.C. Sec. 6501 *et seq.*).

B. The online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children.

C. An online service, product, or feature with advertisements marketed to children.

D. An online service, product, or feature that is substantially similar or the same as an online service, product, or feature subject to subparagraph (B).

E. An online service, product, or feature that has design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music, and celebrities who appeal to children.

F. A significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children.

On appeal, the State argues that this coverage definition does not regulate protected speech; in the State's view, "it does not regulate anything" but rather "clarifies which businesses are subject to the Act's substantive regulatory provisions." NetChoice contends, and the district court concluded, that by virtue of the coverage definition, the Act "burdens speech based on content in *every* application."

The district court held that "[a]pplication of [the enumerated indicators] to determine whether a particular business's online offerings are likely to be accessed by children unavoidably requires an evaluation of content." The district court reasoned that the coverage definition "single[s] out particular subject matter, specifically online content that is likely to be accessed by children" and observed that "[a] business will be treated differently under the CAADCA if it provides online services, products, or features with design elements that are known to be of interest to children, such as games, cartoons, music, or other content that appeals to children, or the business knows that a significant portion of its audience is children." And because it determined any application of the Act's substantive provisions "that do not implicate protected speech" "will be substantially outweighed by the applications of the [substantive provisions] that do implicate protected speech," the district court concluded that NetChoice met the standard for a facial challenge set forth in *Moody*.

We disagree. Unlike the enjoined DPIA report requirement, which "raise[d] the same First Amendment issues" "in every application to a covered business," *NetChoice I*, 113 F.4th at 1116, the coverage definition does not. First, the State persuasively argues that whether "it is reasonable to expect" that a business's "online service, product, or feature would be accessed by children," Cal. Civ. Code § 1798.99.30(b)(4), "says nothing about the nature of the business providing that service, product, or feature." Indeed, as the State proffers, children "are capable of using ride sharing service[s] like Lyft or Waymo, electronic ticketing services such as StubHub or Ticketmaster, financial transaction services such as Paypal or Venmo, fitness products such as NFL Play 60 or Peloton, health-related services such as iHealth, or education-related products such as Wolfram Mathematica." The CAADCA's substantive requirements would "appl[y] evenhandedly" to any of these businesses if they are likely to be accessed by children, regardless of the content available through their online service. . . .

The CAADCA's coverage definition consists of six separately enumerated indicators enabling online businesses to determine whether or not they are subject to the Act. Because each indicator demands different inquiries of online businesses, the coverage definition cannot apply to every online business in the same way. For example, an online business is "likely to be accessed by children" pursuant to indicator (B) where it "is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children." Cal. Civ. Code § 1798.99.30(b)(4)(B). Similarly, a business meets the coverage definition under indicator (F) where "[a] significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children." *Id.* § 1798.99.30(b)(4)(F). Determining whether a service is "routinely accessed by a significant number of children" requires looking to demographic data concerning online traffic to the business's product—that is data *received* by the business, not content the business publishes. *See id.* § 1798.99.30(b)(4)(B). The record establishes—and NetChoice nowhere denies—that frequently, this is data that online businesses already have. *See also NetChoice SB 976*, 152 F.4th at 1022 (concluding that NetChoice's facial challenge to age-verification provisions in California's Protecting Our Kids from Social Media Addiction Act is unripe in part because "NetChoice members can verify users' age in the background without requiring user

input"). The same is true of determining whether "[a] significant amount of the audience" is "children." Cal. Civ. Code § 1798.99.30(b)(4)(F).

However, an online business also comes within the coverage definition if it provides "advertisements marketed to children" or has "design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music, and celebrities who appeal to children." *Id.* § 1798.99.30(b)(4)(C), (E). These indicators may indeed require online businesses to review the content that they publish to determine whether it is directed at or otherwise appealing to children. But that is a different question altogether from whether a significant amount of a business's online patrons are children. A business that satisfies the "significant amount" test would have no need to evaluate whether its product is "directed to children," "marketed to children," or "has design elements that are known to be of interest to children" to determine if the CAADCA applies to it. *Id.* § 1798.99.30(b)(4).

Nowhere does the definition require that all six indicators must be present for the Act to apply, or even that a combination of several factors is required. The content and structure of the provision—listing six separate possible indicators—confirms this reading. For example, indicator (D) defines coverage by reference to businesses "substantially similar" to those satisfying indicator (B) alone, thus creating a derivative category that would be superfluous unless indicator (B) is independently sufficient. Indicators (B) and (F) likewise address the same underlying question—whether children make up a significant share of a platform's audience—but through different evidentiary sources. Reading them as cumulative would allow a business with, for example, substantial company evidence of child users to escape coverage simply by contesting external demographic data, an absurd statutory result. And indicator (A) incorporates COPPA's "directed to children" standard, which overlaps in part with indicators (C) and (E); if all six indicators were required, satisfying (A) alone could never independently trigger coverage, rendering it surplusage. The most natural reading of the provision is that application of any one indicator is sufficient for the business to come within the CAADCA's scope. And because the question that each indicator requires an online business to ask demands a different answer, we cannot say that the coverage definition likely raises the same First Amendment issues in every possible application.

To illustrate the point, recall the State's examples of online services, including ride sharing services, electronic ticketing services, and financial transaction services, all of which may be subject to the CAADCA pursuant to indicators (B) or (F) but which may not otherwise be directed at or marketed to children. NetChoice does not squarely address any of these examples. Instead, NetChoice responds that "the Act does not ask whether minors 'are capable of using' some service" but rather whether the service is likely to be accessed by minors "pursuant to content-based indicia." But NetChoice misreads the coverage definition—which, as explained, does not compel online businesses to apply any potentially content based indicia if the business is routinely accessed by a significant number of children.

It may well be the case that a significant number of children do not routinely access ride sharing services, electronic ticketing services, financial transaction services, or any other online service the State identified. But the district court made no factual findings on those questions, and that information is not otherwise in the record. "The First Amendment analysis is fact intensive and will surely vary from platform to platform." *NetChoice SB 976*, 152 F.4th at 1014 (citation modified). And it is NetChoice's burden to establish that factual record so that the district court could have properly considered every conceivable application of the CAADCA's coverage definition.

NetChoice's focus on applications of the CAADCA that may implicate protected expression does not relieve it from the burden to demonstrate that these applications "substantially outweigh" applications that do not, as *Moody* requires. *NetChoice I*, 113 F.4th at 1115. As we cautioned in *NetChoice I*, "the focus on whether and how these provisions may impact" "social media companies," "without considering any other potential applications, treats

NetChoice's challenges 'more like as-applied claims than like facial ones.' ". "[N]either parties nor courts can disregard the requisite inquiry into how a law works in all of its applications." *Moody*, 603 U.S. at 744.

NetChoice makes the same critical error here. It focuses only on "possible applications" of the coverage definition to companies that publish content, "a subset of the businesses covered by the CAADCA," and "speculate[s] about how that subset of applications could ultimately have a substantial effect on those companies' " protected expression. But in a facial challenge, NetChoice may not "treat[ ] the law[ ] as having certain heartland applications, and mostly confine[ ] the[ ] battle to that terrain." *Moody*, 603 U.S. at 724. . . .

Moreover, in another recent case involving NetChoice, a different panel of our court considered the central coverage definition in California's Protect Our Kids from Social Media Addiction Act, Cal. Health & Safety Code §§ 27000–07, which made the statute applicable "to any internet website including ... a social media platform that personalizes feeds based on information provided by the user." *NetChoice SB 976*, 152 F.4th at 1016 (citation modified). NetChoice argued on appeal that "the Act's focus on social media makes the entire act content based." The panel rejected that argument, explaining that the use of "'social media' platform as statutory shorthand does not render the Act content based, since it applies to websites whether they facilitate social interaction or other forms of content." Accordingly, the "Act as a whole" was not content based by way of its coverage definition. The CAADCA's coverage definition applies even more broadly, regardless of whether an online business publishes content of any kind or none at all.

At bottom, to properly assert a facial challenge, it is NetChoice's burden to establish the CAADCA's "full range" by way of its coverage definition. If NetChoice's prime concern is the CAADCA's effect on social media companies or publishers, it could have brought an as-applied challenge on behalf of some of its members. Instead, NetChoice pursued a more difficult path. That strategic decision "comes at a cost." It requires NetChoice to "develop a record that would allow the court to 'determine [the] law's full set of applications,' cataloging what 'activities, by what actors' the law regulates." We "cannot speculate whether a law unduly burdens expression without a developed record that explains not only how [NetChoice's] platforms work, but also how a wide range of third-party services operate. This information is necessary to characterize the denominator of a law's applications.

To be sure, as we observed in *NetChoice SB 976*, "[d]oing so would entail the 'daunting, if not impossible' task of canvassing how the Act applies to an 'ever-growing number of apps, services, functionalities, and methods for communication and connection.'". We recognized that "such a showing" might be "unrealistic." But we nevertheless stated then, and maintain now, that "[i]t is a mystery how NetChoice could expect to prevail on a facial challenge without candidly disclosing the platforms that it thinks the challenged laws reach" and whether the coverage definition unduly burdens those platforms' expression.

We need not decide today whether any of the coverage definition's enumerated indicators necessarily target expressive activity. "[A]ll we recognize is that some" of the indicators "may be expressive, while others are not, and that inquiry is fact intensive." Because NetChoice stumbles at both steps of the facial analysis, we end our analysis where we began—with *Moody*. Accordingly, we vacate the preliminary injunction with respect to the entire CAADCA and remand for the district court to consider the scope of the CAADCA's coverage definition anew and to weigh any unconstitutional applications against the constitutional ones.

II. NetChoice's challenges to individual provisions are likely to succeed on the merits with respect to the data use and dark patterns restrictions but not the age estimation requirement.

In the alternative to NetChoice's coverage-definition theory, the district court concluded that NetChoice was likely to prevail on its facial challenges to seven individual provisions on

First Amendment or vagueness grounds. The State appeals with respect to the age estimation requirement; the data use restrictions; and the dark patterns restriction; so those are the provisions we consider. We vacate the preliminary injunction order with respect to the age estimation requirement and remand for further consideration. We affirm the preliminary injunction with respect to the four challenged data use restrictions and the dark patterns restriction.

A. NetChoice is not likely to succeed on the merits of its facial challenge to the age estimation requirement.

The CAADCA requires covered businesses to "[e]stimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers." Before the district court, NetChoice challenged this requirement as facially invalid in all applications. The district court rejected the State's argument that "estimating a user's age is conduct, not expressive activity," finding that the requirement that businesses do so "for the purpose of determining what content is appropriate for [children of different] age[s] ... imposes limits on the content a covered business may publish and the content each user may view." The district court applied strict scrutiny and, because it found that age estimation "will require businesses to collect private information that users may not wish to share," concluded that the State had not "met its burden to show that age estimation furthers its interest in the privacy and well-being of children." The district court further held that the State failed to offer any evidence that there were no less restrictive alternatives. As for the *Moody* analysis, the district court found that "the provision will impose the same barriers to speech on all covered businesses and their audiences" and that, "because all applications of § 1798.99.31(a)(5) will impose barriers to protected speech, the provision has no legitimate sweep."

On appeal, the State maintains that the age estimation requirement does not trigger First Amendment scrutiny and that, though the requirement "triggers the Act's other substantive provisions for a particular user," any impact on expressive activity "is the result of the *other substantive provisions* in the Act, not the age estimation requirement." The State further contends that even if the First Amendment applies, the age estimation provision is not content based and, in any event, that it furthers the State's compelling interest in protecting children's privacy and is sufficiently tailored to that goal.

On the record before us, we cannot say that the age estimation requirement facially violates the First Amendment at all, much less in a substantial majority of its applications. For one, it is unclear that the age estimation requirement prevents access to content. The provision requires covered businesses to either "[e]stimate the age of child users with a reasonable level of certainty" or "apply the privacy and data protections afforded to children to all consumers." *Id.* § 1798.99.31(a)(5). On appeal, NetChoice repeats the district court's framing of the provision as "requiring a business to estimate age for the purpose of determining what content is appropriate for that age," but the provision says nothing about restricting content on its face. *See NetChoice I*, 113 F.4th at 1122 (observing that "most of [the provisions NetChoice challenges]," including the age estimation provision, "by their plain language, do not necessarily impact protected speech in all or even most applications"). Rather, it requires covered businesses to apply the Act's privacy and data protections—"half of which," the State points out, "are not even challenged by NetChoice in this suit." The provision is clear that businesses that do not wish to conduct age estimation may publish any content they would like, as long as they default to data and privacy protections for all users. Cal. Civil Code § 1798.99.31(a)(5). We are therefore not convinced that the age estimation provision necessarily burdens protected expression on its face by requiring covered businesses to determine "what content is appropriate" for children.

NetChoice's reading of *Free Speech Coalition v. Paxton*, 606 U.S. 461 (2025), also does not persuade. *Free Speech Coalition* considered a statute that required covered entities to make

adult website visitors submit to an age verification system using either "government-issued identification" or "a commercially reasonable method that relies on public or private transactional data." The Supreme Court observed only that, with respect to that system, there is an "incidental burden that age verification necessarily has on an adult's First Amendment right to access speech that is obscene only to minors." The Court said nothing about the effect of age estimation on First Amendment burdens generally, especially where age estimation is not required as a precondition to access content. To the contrary, the Court observed that "adults have no First Amendment right to avoid age verification, and the [challenged law] can readily be understood as an effort to restrict minors' access."

To the extent NetChoice argues that the age estimation requirement "require[s] consideration of content or proxies for content," *see NetChoice I*, 113 F.4th at 1118, the age estimation requirement may impliedly regulate speech—but we cannot confidently draw that conclusion on this record, either. Recall that the age estimation provision requires "[e]stimat[ing] the age of child users with a reasonable level of certainty appropriate to the risks that arise from the *data management practices* of the business[.]" Cal. Civ. Code § 1798.99.31(a)(5) (emphasis added). The DPIA report provision that we enjoined in *NetChoice I* also required covered businesses to assess "the risks of material detriment to children that arise from the *data management practices* of the business" and required DPIA reports to address several factors, "to the extent applicable," including product design, algorithms, automatic playing of media, and harmful content on the platform. *Id.* § 1798.99.31(a)(1)(B) (emphasis added).

We determined in *NetChoice I* that the "DPIA report requirement regulates the speech of covered businesses and thus triggers review under the First Amendment," and we explained that the enumerated "factors require consideration of content or proxies for content." 113 F.4th at 1118. We rejected the State's argument that the DPIA report requirement "contains no reference to content" but rather "requires a company to mitigate risks from its data management practices." That was because "§ 1798.99.31(a)(2) specifically defines data management practices by reference to the statutory factors a covered business must address under [the DPIA report requirement] when assessing those risks."

To the extent the term "data management practices" in the age estimation provision is also defined by the statutory factors in § 1798.99.31(a)(1)(B), NetChoice may have a reasonable argument that the age estimation provision triggers review under the First Amendment. On the other hand, § 1798.99.31(a)(2) specifically refers to "data management practices of the business identified in the [DPIA] required by [§ 1798.99.31(a)(1)]," while the age estimation requirement does not cross reference § 1798.99.31(a)(1). It is therefore not certain whether "data management practices" takes on its plain meaning with respect to age estimation or whether it impliedly cross-references the statutory factors in § 1798.99.31(a)(1)(B)—which we have read to trigger First Amendment review.

The parties do not develop these arguments, and the district court did not address this precise question. Accordingly, we vacate the preliminary injunction as to the age estimation provision and remand to the district court to consider this question in the first instance. However, we also emphasize that § 1798.99.31(a)(5) allows a covered business to avoid age estimation altogether if it defaults to "apply[ing] the privacy and data protections afforded to children to all consumers." On remand, the parties and the district court may wish to consider the effect of that opt-out language on any burden on expression that may arise from the age estimation requirement.

We also remand for further consideration of the age estimation provision in light of *Moody*. In what must now sound a familiar refrain, "the record needs further development to allow the district court to determine 'the full range of activities the law[ ] cover[s].'" In *NetChoice I*, we made that clear with respect to the CAADCA's age estimation requirement specifically.

Absent a developed record on the various applications of the age estimation requirement—including applications that do not prevent access to content or require data collection for compliance—NetChoice cannot succeed on this facial attack. Likewise, the district court erred by assuming that the only way covered businesses could comply with the provision is by "collect[ing] private information that users may not wish to share," resulting in "businesses ... gather[ing] and creat[ing] a trove of sensitive data regarding children." The State put forth evidence of methods for conducting age estimation that would be acceptable under § 1798.99.31(a)(5) and would require no additional data collection. The district court's discussion of the State's evidence was limited and did not address this point.

Consequently, we cannot determine, from our appellate posture, whether the age estimation requirement facially violates the First Amendment. We vacate the preliminary injunction as to Cal. Civ. Code § 1798.99.31(a)(5).

B. NetChoice is likely to succeed on the merits of its vagueness challenges to the CAADCA's data use restrictions and dark patterns restriction.

We turn next to the preliminary injunction as to the CAADCA's data use restrictions and the dark patterns restriction on constitutional vagueness grounds. "A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012). That principle "requires the invalidation of laws that are impermissibly vague." "A statute can be impermissibly vague ... if it fails to provide people of ordinary intelligence a reasonable opportunity to understand what conduct it prohibits" or "if it authorizes or even encourages arbitrary and discriminatory enforcement." When "vagueness permeates the text" of a law, "it is subject to facial attack." And "[w]hen speech is involved, rigorous adherence to [the void for vagueness doctrine] is necessary to ensure that ambiguity does not chill protected speech."

1. Data Use Provisions

The challenged data use provisions restrict the ways in which, and for what purposes, covered businesses may use a child's personal information. Cal. Civ. Code § 1798.99.31(b)(1)–(4). The relevant provisions state:

> (b) A business that provides an online service, product, or feature likely to be accessed by children shall not take any of the following actions:
>
> > (1) Use the personal information of any child in a way that the business knows, or has reason to know, is *materially detrimental* to the *physical health, mental health, or well-being of a child.*
> >
> > (2) Profile a child by default unless both of the following criteria are met:
> >
> > > (A) The business can demonstrate it has appropriate safeguards in place to protect children.
> > >
> > > (B) Either of the following is true:
> > >
> > > > (i) Profiling is necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which the child is actively and knowingly engaged.
> > > >
> > > > (ii) The business can demonstrate a compelling reason that profiling is in the *best interests* of children.
> >
> > (3) Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature ... unless the business can demonstrate a compelling reason that the collecting, selling,

> sharing, or retaining of the personal information is in the *best interests* of children likely to access the online service, product, or feature.
>
> (4) If the end user is a child, use personal information for any reason other than a reason for which that personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the *best interests* of children.

NetChoice challenged these provisions for their reliance on the undefined terms "material detriment," "best interests," and "well-being." The district court agreed with NetChoice and concluded that these "terms have no established meaning and the CAADCA provides no guidance." It explained that reasonable minds can disagree on what might be detrimental to a child's health or well-being and rejected the State's argument that the "best interests" of a child should be understood similarly to the same "legal term of art that is well-established in family law."

The State contends that "material detriment" and "physical health, mental health, or well-being" each have an accepted plain meaning such that, taken together, the phrase means that "it causes meaningful harm to a child's physical state, mental state, or overall condition of health and happiness." The State cites examples like "using a child's information to connect them to a person that seeks to abuse the child, such as through sexploitation," or "[u]sing a child's information to recommend illegal products such as tobacco, alcohol, or gambling[.]" But these are extreme examples at the margins of what might be materially detrimental to a child's well-being. The more difficult questions arise with examples like sleep loss, distraction, or hurt feelings. As the district court reasoned, and NetChoice argues on appeal, the CAADCA does not provide any guidance as to the breadth of conduct that "material[ ] detriment[ ] to the physical health, mental health, or well-being of a child" may reach. Cal. Civ. Code § 1798.99.31(b)(1). And NetChoice persuasively argues that the risk of subjective enforcement is particularly high because, as it contemplates "material detriment" to "a child," the provision must be assessed as to any single child whose personal information is accessed by a covered online practice. *Cf. NetChoice I*, 113 F.4th at 1120 (observing that the DPIA requirement "that covered businesses opine on whether their services risk 'material detriment to children' " is "vague and onerous").

The State next maintains that the term "best interests of children" should be understood in accordance with California's standard "to determine child custody arrangements, to make guardianship decisions, and in delinquency proceedings." Though, as the district court recognized, the "best interests of the child" standard is clear for the purpose of family law proceedings, the State does not persuasively explain why that case-by-case standard translates to data privacy regulation. On the contrary, the State's reading is incompatible with the data use restrictions' apparent goals. When evaluating the "best interests of the child" in family law proceedings, California courts recognize that "bright line rules in this area are inappropriate" and that "each case must be evaluated on its own unique facts." *In re Marriage of LaMusga*, 32 Cal.4th 1072 (2004). The standard operates through a specific child's circumstances and factual record. The data use restrictions ask something categorically different: covered businesses must determine prospectively whether a given practice is in "the best interests of" not any one child but "*children*"—a class of users that includes every child anywhere who can access a covered online practice. Cal. Civ. Code § 1798.99.31(b)(1)–(4) (emphasis added). Then covered businesses must tailor their practice accordingly. Applied at that scale, without the individualized, highly specific factual record giving the standard meaning in contexts such as a family law case, "best interests of children" cannot provide "sufficient notice of what is proscribed."

The State's argument that the provision's scienter requirement mitigates vagueness is not persuasive. To be sure, "a scienter requirement may mitigate a law's vagueness, especially with respect to the adequacy of notice to the complainant that his conduct is proscribed." Put another way, the "reason to know" language cannot mitigate vagueness where what is

"materially detrimental" to any single child's "well-being" is not clear. Cal. Civ. Code § 1798.99.31(b)(1).

The State contends that "reason to know" is frequently defined to mean "[i]nformation from which a person of ordinary intelligence ... would infer that the fact in question exists or that there is a substantial enough chance of its existence that, if the person exercises reasonable care, the person can assume the fact exists." *Reason To Know*, BLACK'S LAW DICTIONARY (12th ed. 2024); *see also, e.g.*, RESTATEMENT (SECOND) OF TORTS § 12 (1965). And because a business of ordinary intelligence could "base [its] behavior on [its] factual knowledge of the situation at hand and thereby avoid violating the law," the argument goes, the data use prohibitions are clear as to the scope of conduct they regulate. *Jae Gab Kim*, 449 F.3d at 943. But as written, it is not sufficient for a covered business "to be aware only of the objective facts that would fairly put [it] on notice of the use for which" child user data is utilized. . . . The structure of the provision is clear: its mens rea element applies to a covered business's knowledge that the use of the personal information of a child would cause a particular child material harm. Cal. Civ. Code § 1798.99.31(b)(1). Absent any statutory guidance on the meaning of "material[] detriment[]," the provision's scienter requirement does not solve its vagueness.

2. Dark Patterns Restriction

The parties make similar arguments respecting the CAADCA's dark patterns restriction. That provision prohibits covered businesses from:

Us[ing] dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service, product, or feature to forego privacy protections, or *to take any action* that the business knows, or *has reason to know*, is *materially detrimental* to the child's *physical health, mental health, or well-being.*

Cal. Civ. Code § 1798.99.31(b)(7) (emphases added).

The district court found this provision unconstitutionally vague because it does not provide any guidance to covered businesses regarding when they would have "reason to know" that their user interface will have a "materially detrimental" effect on a child's health or well-being. On appeal, the State argues that "dark patterns" is a defined term in the CAADCA[196]; that the phrase "materially detrimental to the child's physical health, mental health, or well-being" has a clear, plain language meaning; and that the provision's mens rea requirement—that the business had "reason to know" its design choice would cause material harm to a child's well-being—mitigates against vagueness.

As with the data use restrictions, the State's plain-meaning argument is unconvincing where the range of harms that could plausibly qualify as "materially detrimental" is vast, spanning everything from financial exploitation to sleep loss, distraction, or hurt feelings. The fact that "dark pattern" is a defined term in the CAADCA does not help a covered business distinguish between these harms. And the prohibition's use of the singular "child," like in the data use restrictions, suggests that it is actionable based on a single child's response to an online interface, meaning that a business designing a product accessed by millions of child users could face liability whenever any one of them experiences a harm that a regulator deems "material." Businesses of ordinary intelligence cannot reliably determine what compliance requires.

We therefore affirm the district court's injunction with respect to the data use and dark patterns restrictions on vagueness grounds.

---

[196] The Act incorporates a definition of a "dark pattern" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation." Cal. Civ. Code § 1798.140(*l*); *id.* § 1798.99.30(a).

CONCLUSION

For the foregoing reasons, we **AFFIRM** the district court's preliminary injunction insofar as it enjoined enforcement of California Civil Code §§ 1798.99.31(b)(1)–(4) and 1798.99.31(b)(7), and **VACATE** the remainder of the preliminary injunction.

Notes

1.) CAADCA passed the California legislature unanimously, yet this is not always a sign of a well-considered law. Even as the court rejects the broadest possible challenges brought by NetChoice, it still recognizes that much about the law is loosely drafted. Imagine one did have to comply with the data use restrictions. How difficult would it be to draft corporate policy to accomplish those aims? Is it materially detrimental to feed a child a steady diet of obesity-shaming content? Quite possibly; that was likely the kind of thing the legislature had in mind. What about a steady diet of religious content? Or irreligious content? Or content that encourages excessive toy-buying? One could imagine good-faith arguments that all of those are harmful to children, at least absent moderation.

2.) Whenever age gating, age verification, or age tailoring is proposed, there is a concern that protecting children from a particular form of content will come at the expense of stopping adults from being able to access that content. This commonly comes up in the context of pornography, where sometimes this overbreadth may be part of the point. In 2025, the Supreme Court upheld a Texas law requiring certain commercial websites that publish sexually explicit content to verify the ages of those seeking access. Though adults have a First Amendment right to be able to access such content – assuming it is not obscene to them – requiring them to verify their ages is an acceptable burden on that right. *Free Speech Coal., Inc. v. Paxton*, 606 U.S. 461 (2025).

3.) On the idea of giving all users the privacy protections granted to children: Giving all users *content* appropriate to children is deeply problematic: imagine moderating a discussion of foreign policy such that it would be appropriate to first graders. But there are foreign jurisdictions that give privacy protections to adults that exceed those granted to children by COPPA and CAADCA. The extent to which American businesses could grant those protections to American adults in an economically viable way is unclear, but it is certainly technically feasible.

C. Marketing Privacy

In addition to the sectoral privacy statutes that regulate large parts of the American economy and common uses of technology—such as HIPAA, GLBA, FCRA, and ECPA—there is also a collection of more minor sectoral statutes. The dividing line between major and minor is somewhat unclear. Each of the statutes in this section is decidedly minor, however. Each was intended to address a specific narrow problem and the statutes generally do not matter outside the context of that problem, though clever plaintiffs do try to assert that they matter more broadly.

1) CAN-SPAM Act

The CAN-SPAM Act, 15 U.S.C. § 7701, is never referred to by its full name, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. As the name implies, it was aimed at saving people from being pestered by unwanted commercial messages, particularly those that were pornographic. The Act does not forbid marketing communications, but it does set rules that prohibit various kinds of deception in electronic marketing, as well as rules that require consumers be given the ability to opt out. If one is thinking in terms of the traditional privacy torts, one might view this as a form of intrusion upon seclusion protection.

The CAN-SPAM Act outlaws certain commercial email acts and practices. For example, the Act prohibits transmission of any email that contains false or misleading header or "from" line information. Messages must also contain either a functioning return email address or similar Internet-based mechanism for recipients to use to "opt out" of receiving future commercial email messages. Neither the sender, or others acting on the sender's behalf, may initiate a commercial email to a recipient more than ten business days after the recipient has opted out. Senders cannot charge a fee for opting out or sell the consumer's information after they have opted out. The opt-out mechanism must not take more than a single step for the consumer (*i.e.,* a single email request or a single visit to a single webpage to change marketing communications preferences).

The Act requires three disclosures to be made in sending commercial email messages: (1) clear and conspicuous identification that the message is an advertisement or solicitation, (2) clear and conspicuous notice of the opportunity to decline to receive further commercial email messages from the sender, and (3) a valid physical postal address of the sender. 15 U.S.C. § 7704(a)(5).

In the world of CAN-SPAM, there are three types of information that an email can contain: "commercial content which advertises or promotes a commercial product or service, including content on a website operated for a commercial purpose; transactional or relationship content which facilitates an already agreed-upon transaction or updates a customer about an ongoing transaction; [and] other content which is neither a commercial nor transactional or relationship."[197] The Act applies to messages that have a primary commercial purpose, meaning they are primarily aimed at commercial advertisement as opposed to something else. Simply put, "[I]f the subject line would lead the recipient to think it's a commercial message, it's a commercial message for CAN-SPAM purposes."[198] So an Amazon email about upcoming "Prime Day" sales is a commercial message under CAN-SPAM. An Amazon email entitled "Order Summary" that also contains product advertisements under your order summary is not.

As with COPPA, the CAN-SPAM Act is primarily enforced by the Federal Trade Commission and state attorney generals; there is no private right of action. ISPs can bring suit, however, given their particular role in delivering and hosting internet communications. Civil damages are possible for first violations, with per message costs (which differ for all categories of plaintiffs) and set maximums for state attorney generals (two million dollars) and ISPs (one million dollars).

CAN-SPAM has somewhat broader application than might be immediately apparent as it applies not just to traditional email, but also to other forms of electronic messaging, including email-to-text messaging. In *MySpace, Inc. v. The Globe.com,* CV 06-3391-RGK, 2007 WL 1686966 (C.D. Cal. Feb. 27, 2007) TheGlobe made at least ninety-five dummy accounts and sent almost 400,000 unsolicited commercial messages to MySpace users through the MySpace messaging system. The Central District of California said that direct messages sent to MySpace users' inboxes counted as "electronic mail messages," which CAN-SPAM Act defined as messages sent to a "unique electronic mail address" with a "destination . . . to which an electronic mail message can be sent or delivered." Each MySpace user account had a unique URL, satisfying the first prong, and the MySpace website was the message's destination, satisfying the second prong. This was only one of several such cases. *See also MySpace, Inc. v. Wallace* 498 F. Supp. 2d 1293, 1300 (C.D. Cal. 2007) and *Facebook, Inc. v. MaxBounty, Inc.*, 274 F.R.D. 279, 283-4 (N.D. Cal. 2011).

---

[197] FEDERAL TRADE COMMISSION, CAN-SPAM ACT: A COMPLIANCE GUIDE FOR BUSINESS (Jan. 2024), https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business.

[198] *Id.*

2) Telephone Consumer Protection Act

As CAN-SPAM was aimed at unwanted electronic messages, the Telephone Consumer Protection Act of 1991 (TCPA), 47 U.S.C. § 227, was aimed at unwanted telephone calls. Specifically, it regulates telemarketing and the use of automatic dialers.

Scope. The TCPA regulates unsolicited calls, meaning calls from a telemarketer to a prospective customer with whom the telemarketer does not have an existing relationship and from whom the telemarketer has not obtained consent. The key scope limitation is that the TCPA only applies to calls "made for a commercial purpose."

Enforcement. The TCPA can be enforced by the state both civilly and criminally, with possible criminal fines up to $10,000 per violation. There is also a private right of action allowing for individuals to sue in state or federal court for $500 per violation, or three times that if the violation is willful or knowing. Jurisdiction for civil actions is exclusive to the federal courts.

Affirmative Defense. Telemarketers can offer as an affirmative defense that they established "reasonable practices and procedures to effectively prevent telephone solicitations in violation of the regulations prescribed under this subsection."

Prohibitions on Prerecorded Messages and Automatic Dialers. Callers cannot dial a cellphone, hospital phone, paging service, or various emergency lines with automatic dialing devices, and cannot make calls to any of those or to residential landlines that use an artificial or prerecorded voice without the recipient's consent.

Fax Machines. The TCPA prohibits the use of a fax, computer, or other device to send an unsolicited advertisement to a fax machine.

D. Tracking Privacy

1) ECPA and Online Tracking

Though the Electronic Communications Privacy Act is often considered in terms of government investigations (see Chapter 3.D), its civil component is also extremely important. The below case is part of a recent wave of litigation that attempts to use the ECPA to regulate online tracking via cookies. This litigation has had mixed success, as the opinion makes plain.

In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589 (9th Cir. 2020)

THOMAS, Chief Judge:

Facebook uses plug-ins to track users' browsing histories when they visit third-party websites, and then compiles these browsing histories into personal profiles which are sold to advertisers to generate revenue. The parties do not dispute that Facebook engaged in these tracking practices after its users had logged out of Facebook.

Facebook facilitated this practice by embedding third-party plug-ins on third-party web pages. The plug-ins, such as Facebook's "Like" button, contain bits of Facebook code. When a user visits a page that includes these plug-ins, this code is able to replicate and send the user data to Facebook through a separate, but simultaneous, channel in a manner undetectable by the user.

As relevant to this appeal, the information Facebook allegedly collected included the website's Uniform Resource Locator ("URL") that was accessed by the user. URLs both identify an internet resource and describe its location or address. "[W]hen users enter URL addresses

into their web browser using the 'http' web address format, or click on hyperlinks, they are actually telling their web browsers (the client) which resources to request and where to find them. Thus, the URL provides significant information regarding the user's browsing history, including the identity of the individual internet user and the web server, as well as the name of the web page and the search terms that the user used to find it. In technical parlance, this collected URL is called a "referer header" or "referer." Facebook also allegedly collected the third-party website's Internet Protocol ("IP") address, which reveals only the owner of the website.

Facebook allegedly compiled the referer headers it collected into personal user profiles using "cookies"—small text files stored on the user's device. When a user creates a Facebook account, more than ten Facebook cookies are placed on the user's browser. These cookies store the user's login ID, and they capture, collect, and compile the referer headers from the web pages visited by the user. As most relevant to this appeal, these cookies allegedly continued to capture information after a user logged out of Facebook and visited other websites.

Plaintiffs filed a consolidated complaint on behalf of themselves and a putative class of people who had active Facebook accounts between May 27, 2010 and September 26, 2011. Plaintiffs filed an amended complaint. In the amended complaint, they alleged a number of claims. The claims relevant to this appeal consist of: (1) violation of the Wiretap Act, 18 U.S.C. § 2510, *et seq.*; (2) violation of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701; (3) violation of the California Invasion of Privacy Act ("CIPA"), Cal. Pen. Code §§ 631, 632; (4) invasion of privacy; (5) intrusion upon seclusion; (6) breach of contract; (7) breach of the duty of good faith and fair dealing . . . .

II

To establish standing, a "[p]laintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo v. Robins* (2016). To establish an injury in fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized." A particularized injury is one that affects the plaintiff in a "personal and individual way."

A concrete injury is one that is "real and not abstract." *Spokeo*. Although an injury "must be 'real' and 'not abstract' or purely 'procedural' . . . it need not be 'tangible.'" Indeed, though a bare procedural violation of a statute is insufficient to establish an injury in fact, Congress may "elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate" to confer standing. *Spokeo*.

To determine whether Congress has done so, we ask whether: (1) "Congress enacted the statute at issue to protect a concrete interest that is akin to a historical, common law interest[,]" and (2) the alleged procedural violation caused real harm or a material risk of harm to these interests.

A

As to the statutory claims, the legislative history and statutory text demonstrate that Congress and the California legislature intended to protect these historical privacy rights when they passed the Wiretap Act, SCA, and CIPA. *See* S. Rep. No. 99-541 (1986) ("[The Wiretap Act] is the primary law protecting the security and privacy of business and personal communications in the United States today. [The SCA] is modeled after the Right to Financial Privacy Act to protect privacy interests in personal and proprietary information . . . . "); Cal. Pen. Code § 630 (noting that CIPA was passed "to protect the right of privacy of the people of this state"). Thus, these statutory provisions codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing.

Plaintiffs have adequately alleged harm to these privacy interests. Plaintiffs alleged that Facebook continued to collect their data after they had logged off the social media platform, in order to receive and compile their personally identifiable browsing history. As alleged in the complaint, this tracking occurred "no matter how sensitive" or personal users' browsing histories were. Facebook allegedly constantly compiled and updated its database with its users' browsing activities, including what they did when they were not using Facebook. According to Plaintiffs, by correlating users' browsing history with users' personal Facebook profiles—profiles that could include a user's employment history and political and religious affiliations—Facebook gained a cradle-to-grave profile without users' consent.

B

Plaintiffs also alleged theories of California common law trespass to chattels and fraud, statutory larceny, and violations of the CDAFA [Computer Data Access and Fraud Act]. The district court dismissed these claims for lack of standing, concluding that the Plaintiffs failed to demonstrate that they had suffered the economic injury the district court viewed as necessary to bring each of these claims. We respectfully disagree.

Plaintiffs allege that Facebook is unjustly enriched through the use of their data. Facebook argues that unjust enrichment is not sufficient to confer standing, and that Plaintiffs must instead demonstrate that they either planned to sell their data, or that their data was made less valuable through Facebook's use.

However, "state law can create interests that support standing in federal courts." *Cantrell v. City of Long Beach* (9th Cir. 2001). As relevant here, California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss.

In other words, California law requires disgorgement of unjustly earned profits regardless of whether a defendant's actions caused a plaintiff to directly expend his or her own financial resources or whether a defendant's actions directly caused the plaintiff's property to become less valuable.

Because California law recognizes a legal interest in unjustly earned profits, Plaintiffs have adequately pleaded an entitlement to Facebook's profits from users' personal data sufficient to confer Article III standing. Plaintiffs allege that their browsing histories carry financial value. They point to the existence of a study that values users' browsing histories at $52 per year, as well as research panels that pay participants for access to their browsing histories.

III

A

Plaintiffs adequately stated claims for relief for intrusion upon seclusion and invasion of privacy under California law. To state a claim for intrusion upon seclusion under California common law, a plaintiff must plead that (1) a defendant "intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy[,]" and (2) the intrusion "occur[red] in a manner highly offensive to a reasonable person."

A claim for invasion of privacy under the California Constitution involves similar elements. Plaintiffs must show that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is "so serious . . . as to constitute an egregious breach of the social norms" such that the breach is "highly offensive."

Because of the similarity of the tests, courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive. We address both in turn.

1

We first consider whether a defendant gained "unwanted access to data by electronic or other covert means, in violation of the law or social norms." To make this determination, courts consider a variety of factors, including the customs, practices, and circumstances surrounding a defendant's particular activities.

Thus, the relevant question here is whether a user would reasonably expect that Facebook would have access to the user's individual data after the user logged out of the application. Facebook's privacy disclosures at the time allegedly failed to acknowledge its tracking of logged-out users, suggesting that users' information would not be tracked.

The applicable Facebook Statement of Rights and Responsibilities ("SRR") stated:

> Your privacy is very important to us. We designed our Privacy Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Privacy Policy, and to use it to make informed decisions.

SRR, dated April 26, 2011.

Facebook's applicable Data Use Policy, in turn, stated:

> We receive data whenever you visit a game, application, or website that uses [Facebook's services]. This may include the date and time you visit the site; the web address, or URL, you're on; technical information about the IP address, browser and the operating system you use; and, *if you are logged in to Facebook,* your user ID.

Data Use Policy, dated September 7, 2011 (emphasis added).

Finally, Facebook's "Help Center" at the time included answers to questions related to data tracking. Most relevantly, one answer from a Help Center page at the time answered the question "[w]hat information does Facebook receive about me when I visit a website with a Facebook social plug in?" The Help Center page first stated that Facebook collected the date and time of the visit, the referer URL, and other technical information. It continued, "[i]f you are logged into Facebook, we also see your user ID number and email address. If you log out of Facebook, we will not receive this information about partner websites but you will also not see personalized experiences on these sites."

Plaintiffs have plausibly alleged that an individual reading Facebook's promise to "make important privacy disclosures" could have reasonably concluded that the basics of Facebook's tracking—when, why, and how it tracks user information—would be provided. Plaintiffs have plausibly alleged that, upon reading Facebook's statements in the applicable Data Use Policy, a user might assume that only logged-in user data would be collected. Plaintiffs have alleged that the applicable Help Center page affirmatively stated that logged-out user data would not be collected. Thus, Plaintiffs have plausibly alleged that Facebook set an expectation that logged-out user data would not be collected, but then collected it anyway.

In addition, the amount of data allegedly collected was significant. Plaintiffs allege that "[n]o matter how sensitive the website, the referral URL is acquired by Facebook along with the cookies that precisely identify the [logged-out] user" and that Facebook acquires an "enormous amount of individualized data" through its use of cookies on the countless websites that incorporate Facebook plug-ins.

In light of the privacy interests and Facebook's allegedly surreptitious and unseen data collection, Plaintiffs have adequately alleged a reasonable expectation of privacy. Case law supports this determination. In *In re Google, Inc. Cookie Placement Consumer Privacy Litigation* (3d Cir. 2015)—where the Third Circuit similarly interpreted California Law—the

court held that users maintained a reasonable expectation of privacy in their browsing histories when Google tracked URLs after the users denied consent for such tracking. That users in those cases explicitly denied consent does not render those cases distinguishable from the instant case, given Facebook's affirmative statements that it would not receive information from third-party websites after users had logged out. Indeed, in those cases, the critical fact was that the online entity represented to the plaintiffs that their information would not be collected, but then proceeded to collect it anyway.

The nature of the allegedly collected data is also important. Plaintiffs allege that Facebook obtained a comprehensive browsing history of an individual, no matter how sensitive the websites visited, and then correlated that history with the time of day and other user actions on the websites visited. This process, according to Plaintiffs, resulted in Facebook's acquiring "an enormous amount of individualized data" to compile a "vast repository of personal data."

Contrary to Facebook's arguments, this case can also be distinguished from *U.S. v. Forrester* (9th Cir. 2008) and *In re Zynga Privacy Litigation* (9th Cir. 2014) as it relates to an analysis of a reasonable expectation of privacy. In *Forrester*, we considered whether the individuals had a reasonable expectation of privacy in "the to/from addresses of their messages or the IP addresses of the websites they visit." Concluding that users did not maintain a reasonable expectation of privacy in such information, we determined that users "should know that this information is provided to and used by Internet service providers for the specific purposes of directing the routing information." But, in a footnote, we went on to distinguish the IP addresses collected in *Forrester* from the collection of URLs, which we stated "might be more constitutionally problematic," explaining that, "[a] URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity."

In *Zynga*, the plaintiffs relied on this footnote to argue that they maintained a reasonable expectation of privacy in the URLs of gaming websites collected without their knowledge and disclosed to third parties by Zynga (a gaming platform) and Facebook. The *Zynga* plaintiffs alleged that users would log in to their Facebook account and "then click on the Zynga game icon within the Facebook interface." Facebook and Zynga would then collect a referer header containing the URL for the Zynga game, after which the Zynga server would load the game in a small frame embedded on the Facebook website. According to the *Zynga* plaintiffs, "Zynga programmed its gaming applications to collect the information provided in the referer header, and then transmit this information to advertisers and other third parties."

In *Zynga*, we concluded that the collected information was not problematic because it differed from the URLs containing sensitive information alluded to in *Forrester*'s footnote. We determined that "[i]nformation about the address of the Facebook webpage the user was viewing is distinguishable from the sort of communication involving a search engine discussed in *Forrester*." We then continued to say that "a Google search URL not only shows that a user is using the Google search engine, but also shows the specific search terms the user had communicated to Google."

Here, Plaintiffs allege that Facebook collects a full-string detailed URL, which contains the name of a website, folder and sub-folders on the web-server, and the name of the precise file requested. Their complaint notes that a user might type a search term into Google's search engine, which would return a link to an article relevant to the search term.

In sum, Plaintiffs have sufficiently pleaded a reasonable expectation of privacy to survive a Rule 12(b)(6) motion to dismiss.

2

However, in order to maintain a California common law privacy action, "[p]laintiffs must show more than an intrusion upon reasonable privacy expectations. Actionable invasions of

privacy also must be 'highly offensive' to a reasonable person, and 'sufficiently serious' and unwarranted so as to constitute an 'egregious breach of the social norms.'" Determining whether a defendant's actions were "highly offensive to a reasonable person" requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive.

The ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage. Indeed, Plaintiffs have alleged that internal Facebook communications reveal that the company's own officials recognized these practices as a problematic privacy issue.

B

Plaintiffs also have sufficiently alleged that Facebook's tracking and collection practices violated the Wiretap Act and CIPA.

1

The Wiretap Act prohibits the unauthorized "interception" of an "electronic communication." Similarly, CIPA prohibits any person from using electronic means to "learn the contents or meaning" of any "communication" "without consent" or in an "unauthorized manner." Both statutes contain an exemption from liability for a person who is a "party" to the communication, whether acting under the color of law or not. Courts perform the same analysis for both the Wiretap Act and CIPA regarding the party exemption.

The party exception must be considered in the technical context of this case. When an individual internet user visits a web page, his or her browser sends a message called a "GET request" to the web page's server. The GET request serves two purposes: it first tells the website what information is being requested and then instructs the website to send the information back to the user. The GET request also transmits a referer header containing the personally identifiable URL information. Typically, this communication occurs only between the user's web browser and the third-party website. On websites with Facebook plug-ins, however, Facebook's code directs the user's browser to copy the referer header from the GET request and then send a separate but identical GET request and its associated referer header to Facebook's server. It is through this duplication and collection of GET requests that Facebook compiles users' browsing histories.

The Wiretap Act does not define the term "party" in its liability exemption, and the other circuit courts that have considered the Act's scope have interpreted the term in different ways. The First and Seventh Circuits have implicitly assumed that entities that surreptitiously duplicate transmissions between two parties are not parties to communications within the meaning of the Act. In *In re Pharmatrak, Inc. Privacy Litigation* (1st Cir. 2003), the First Circuit considered whether the defendant could face liability under the Wiretap Act when it employed software that "automatically duplicated part of the communication between a user and a [third-party website] and sent this information to [the defendant]." The First Circuit rejected the defendant's argument that "there was no interception because 'there were always two separate communications: one between the Web user and the [third-party website], and the other between the Web user and [the defendant].'" Noting that the defendant "acquired the same URL . . . exchanged as a part of the communication between the [third-party website] and the user," it determined that the defendant's acquisition constituted an interception and could still render it liable.

In *United States v. Szymuszkiewicz* (7th Cir. 2010), the Seventh Circuit reached a similar conclusion. In that case, the Seventh Circuit considered whether a defendant violated the Wiretap Act when he employed a software that instructed his employer's email to duplicate and forward all emails the employer received to the defendant's own inbox. The court

determined that, because the copies were sent contemporaneously with the original emails, the defendant had intercepted the communications and could be held liable.

However, the Third Circuit has held to the contrary. In *In re Google Cookie*, the court considered whether internet advertising companies were parties to a communication when they placed cookie blockers on web-users' browsers to facilitate online advertisements. As in the instant case, the users sent GET requests to third-party websites and upon receipt, the website would duplicate the GET request and send it to the defendants. The Third Circuit concluded that the defendants were "the intended recipients" of the duplicated GET requests, and thus "were parties to the transmissions at issue."

We adopt the First and Seventh Circuits' understanding that simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception. As we have previously held, the "paramount objective of the [Electronic Communications Privacy Act, which amended the Wiretap Act] is to protect effectively the privacy of communications." We also recognize that the Wiretap Act's legislative history evidences Congress's intent to prevent the acquisition of the contents of a message by an unauthorized third-party or "an unseen auditor." Permitting an entity to engage in the unauthorized duplication and forwarding of unknowing users' information would render permissible the most common methods of intrusion, allowing the exception to swallow the rule.

Therefore, we conclude that Facebook is not exempt from liability as a matter of law under the Wiretap Act or CIPA as a party to the communication. We do not opine whether the Plaintiffs adequately pleaded the other requisite elements of the statutes, as those issues are not presented on appeal.

C

The district court properly dismissed Plaintiffs' SCA claims. The SCA requires Plaintiffs to plead that Facebook (1) gained unauthorized access to a "facility" where it (2) accessed an electronic communication in "electronic storage."

Electronic storage is defined as either the "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

Plaintiffs allege that "[w]eb-browsers store a copy of the Plaintiffs' URL requests in the toolbar while the user remains present at a particular webpage," and that this storage is incidental to the electronic communication because once "the user hits the Enter button or clicks on a link, the communication is in the process of being sent and received between the user and the first-party website." Plaintiffs similarly assert that their browsing history—a record of previously viewed websites—serves purposes of "backup protection" of such communications. In short, Plaintiffs allege that the URL is in "electronic storage" in the toolbar during the split-second that it takes to complete a search. In Plaintiffs' view, because Facebook duplicates the URL and sends it to its servers during that split second, it accesses the URL while it is in this "electronic storage."

The district court considered the GET requests that Facebook duplicated and forwarded to its servers as wholly separate from the copy of the URL displayed in the search toolbar. Because the copy in the toolbar was not stored "incident to transmission" but was only present for the user's convenience, the district court determined that the Plaintiffs' data was not in electronic storage.

We agree. The communications in question—the GET requests themselves—are not the communications stored in the user's toolbar. Rather, the GET requests are sent directly between the user and the third-party website. The text displayed in the toolbar serves only as a visual indication—a means of informing the user—of the location of their browser. Thus, the

URL's appearance in the toolbar is not "incidental" to the transmission of the URL or GET request.

What is more, Plaintiffs' interpretation of the SCA would stretch its application beyond its limits. True, the SCA's legislative history suggests that Congress intended the term "electronic storage" to be broadly construed, and not limited to "particular mediums, forms, or locations." Nonetheless, the text and legislative history of the SCA demonstrate that its 1986 enactment was driven by congressional desire to protect third-party entities that stored information on behalf of users. Since then, the SCA has typically only been found to apply in cases involving a centralized data-management entity; for instance, to protect servers that stored emails for significant periods of time between their being sent and their recipients' reading them. Here, the allegations, even construed in the light most favorable to Plaintiffs, do not show that the communications were even in "storage," much less that the alleged "storage" within a URL toolbar falls within the SCA's intended scope.

D

The district court also properly held that the Plaintiffs have not stated a breach of contract claim. In order to establish a contract breach, Plaintiffs must allege: (1) the existence of a contract with Facebook, (2) their performance under that contract, (3) Facebook breached that contract, and (4) they suffered damages.

Plaintiffs allege that Facebook entered into a contract with each Plaintiff consisting of the SRR, Privacy Policy, and relevant Help Center pages. The parties agree that the SRR constitutes a contract. This document states "[y]our privacy is very important to us" and "[w]e encourage you to read the Privacy Policy, and to use it to help make informed decisions." But this document does not contain an explicit promise not to track logged-out users. For that allegation, Plaintiffs instead rely on language from the Data Use Policy and the Help Center pages.

To properly incorporate another document, the document "need not recite that it incorporates another document, so long as it guide[s] the reader to the incorporated document." The attached SRR does not reference a Data Use Policy and thus, it does not guide the reader to the incorporated document on which Plaintiffs rely. As such, as a matter of law, any promise not to track logged-out users therein was not incorporated.

Notes

1. Consider why the ECPA is so important here. Though one can allege an intrusion upon seclusion and argue many of the same elements, the ECPA has extensive statutory damages. If, as seems likely, the actual damages of this tracking are hard to quantify and relatively small, then the ECPA's statutory damages provide most of the value of this litigation.
2. Defendants in these cases often argue that the ECPA was never intended to be about this kind of tracking and monitoring. Certainly this is the case historically. The last substantial revision of the ECPA was in 1986, which predates the rise of the internet as a major tool of consumer communication. But that does not mean the statute should not apply to new and changing technology. Reading these cases, however, it is important to remember that defendants view them as blatant money-grabs, a misuse of a statute whose damages were calibrated for tapping of telephone calls. On that point, this case settled in 2022 for 90 million dollars, of which 26 million went to attorney fees. *In re Facebook Internet Tracking Litig.*, No. 5:12-MD-02314-EJD, 2022 WL 16902426, at *2 (N.D. Cal. Nov. 10, 2022).

2) Video Privacy Protection Act

The Video Privacy Protection Act (VPPA) has raised a number of awkward questions in the post-Blockbuster age.[199] Challenges under the VPPA have been brought against a number of websites that either operate video-streaming services—and look very much like old-school video rental stores—or include video elements on sites focused on other content or business models. The below case addresses the question of what counts as disclosing personal information under the Act.

In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 (3rd Cir. 2016)

FUENTES, Circuit Judge:

This is a multidistrict consolidated class action. The plaintiffs are children younger than 13 who allege that the defendants, Viacom and Google, unlawfully collected personal information about them on the Internet, including what webpages they visited and what videos they watched on Viacom's websites. Many of the plaintiffs' claims overlap substantially with those we addressed in *In re Google Inc. Cookie Placement Consumer Privacy Litigation* (2015), and indeed fail for similar reasons. Even so, two of the plaintiffs' claims—one for violation of the federal Video Privacy Protection Act, and one for invasion of privacy under New Jersey law—raise questions of first impression in our Circuit.

The Video Privacy Protection Act, passed by Congress in 1988, prohibits the disclosure of personally identifying information relating to viewers' consumption of video-related services. Interpreting the Act for the first time, we hold that the law permits plaintiffs to sue only a person who *discloses* such information, not a person who *receives* such information. We also hold that the Act's prohibition on the disclosure of personally identifiable information applies only to the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior. In our view, the kinds of disclosures at issue here, involving digital identifiers like IP addresses, fall outside the Act's protections.

The plaintiffs also claim that Viacom and Google invaded their privacy by committing the tort of intrusion upon seclusion. That claim arises from allegations that Viacom explicitly promised not to collect any personal information about children who browsed its websites and then, despite its assurances, did exactly that. We faced a similar allegation of deceitful conduct in *Google*, where we vacated the dismissal of state-law claims for invasion of privacy and remanded them for further proceedings. We reach a similar result here, concluding that, at least as to Viacom, the plaintiffs have adequately alleged a claim for intrusion upon seclusion.

Accordingly, we will affirm the District Court's dismissal of most of the plaintiffs' claims, vacate its dismissal of the claim for intrusion upon seclusion against Viacom, and remand the case for further proceedings.

Internet Cookie Technology

When a person uses a web browser to access a website, the browser sends a "GET" request to the server hosting that site. So, for example, if a person types "www.nick.com" into the address bar of his or her web browser, the browser contacts the server where Nick.com is hosted and transmits data back to the user's computer. In addition to other content, Nick.com may also display ads from third parties. These ads typically reside on a different server. To display the ad, the Nick.com server will direct the user's browser to send another "GET" request to the third-party server, which will then transmit the ad directly to the user's computer. From the user's perspective, all of this appears to happen simultaneously, and all the visual

[199] Blockbuster was a leading videotape, DVD, and Blu-ray rental service prior to the rise of streaming services. It operated 9,094 stores in 2004. In 2024, it operated 1.

information on Nick.com appears to originate from a single source. In reality, the Nick.com website is an assemblage of content from multiple servers hosted by different parties.

An Internet "cookie" is a small text file that a web server places on a user's computing device. Cookies allow a website to "remember" information about a user's browsing activities (such as whether or not the user is logged-in, or what specific pages the user has visited). We can distinguish between first-party cookies, which are injected into a user's computer by a website that the user chooses to visit (*e.g.*, Nick.com), and third-party cookies, which are placed on a user's computer by a server other than the one that a person intends to visit (*e.g.*, by an ad company like Google).

Advertising companies use third-party cookies to help them target advertisements more effectively at customers who might be interested in buying a particular product. Cookies are particularly powerful if the same company hosts ads on more than one website. In those circumstances, advertising companies are able to follow a user's browsing habits across multiple websites that host the company's ads. Given Google's dominance in the Internet advertising market, the plaintiffs claim that Google is able to use cookies to track users' behavior across large swaths of the Internet.

Factual Allegations

Defendant Viacom owns the children's television station Nickelodeon. It also operates Nick.com, a website geared towards children that offers streaming videos and interactive games. A child registers to use Nick.com by signing up for an account and choosing a username and password. During the registration process, a child provides his or her birthdate and gender to Viacom, and Viacom then assigns the child a code based on that information. The plaintiffs also assert that Viacom's registration form includes a message to children's parents: "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!"

The plaintiffs allege that Viacom and Google unlawfully used cookies to track children's web browsing and video-watching habits on Viacom's websites. They claim that the defendants collected information about children in at least four ways.

First, when a user visits one of Viacom's websites, Viacom places its own first-party cookie on that user's computer. This permits Viacom to track a child's behavior, including which games a child plays and which videos a child watches.

Second, Google contracts with Viacom to place advertisements on Viacom's websites. As a result, Google is able to place third-party cookies on the computers of persons who visit those websites, including children.

Third, the plaintiffs claim that, "[u]pon information and belief, Viacom also provided Google with access to the profile and other information contained within Viacom's first-party cookies."

Fourth, the plaintiffs assert that, once Google places a cookie on a person's computer, it can track that person across any website on which Google displays ads. Google uses so-called "Doubleclick.net cookies" to accomplish this task. In addition, Google offers its own collection of online services to Google account-holders and other web users, including Gmail, Google Maps, and YouTube (which Google owns). The plaintiffs claim that Google combines information that it collects from people using *its* websites with information it gleans from displaying ads on *others'* websites. They also claim that "Viacom is aware of Google's ubiquitous presence on the Internet and its tracking of users."

A. The Video Privacy Protection Act

Congress passed the Video Privacy Protection Act in 1988 after the *Washington City Paper* published Supreme Court nominee Robert Bork's video rental history. "The paper had

obtained (without Judge Bork's knowledge or consent) a list of the 146 films that the Bork family had rented from a Washington, D.C.-area video store." According to the Senate Report accompanying the law's passage, Congress passed the Act "[t]o preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials."

The Act creates a private cause of action for plaintiffs to sue persons who disclose information about their video-watching habits. Unfortunately, as the Seventh Circuit has noted, the Act "is not well drafted," requiring us to begin by summarizing a bit of legislative jargon. The Act defines several key terms:

• **Consumer:** "any renter, purchaser, or subscriber of goods or services from a video tape service provider."

• **Video tape service provider:** "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials."

• **Personally identifiable information:** "includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."

To state a claim under the Act, a plaintiff must allege that "[a] video tape service provider . . . knowingly disclose[d], to any person, personally identifiable information concerning any consumer of such provider." The Act (i) sets a minimum penalty of $2,500 per violation, (ii) permits a plaintiff to recover punitive damages, reasonable attorneys' fees, and litigation costs, and (iii) empowers district courts to provide appropriate equitable relief.

The plaintiffs allege that Viacom disclosed to Google URL information that effectively revealed what videos they watched on Nickelodeon's websites, and static digital identifiers (such as IP addresses, browser fingerprints, and unique device identifiers) that enabled Google to link the watching of those videos to their real-world identities. They bring claims under the Act against both defendants.

1. Whether Google is an Appropriate Defendant under the Act

The first question we confront is whom, exactly, the Act permits the plaintiffs to sue. The plaintiffs contend that the Act allows them to sue *both* a video tape service provider who discloses personally identifiable information *and* a person who receives that information. To put it another way, the parties seem to agree that the video clerk who leaked Judge Bork's rental history clearly would have been liable under the Act had it been in force at the time—but what about the reporter at the *Washington City Paper* to whom he leaked the information? The plaintiffs say he would have been liable as well. Google (standing-in for the reporter in our fact pattern) disagrees.

The text of the statute is not clear on this point. Subsection (b) states that a "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (c)." Subsection (c), in turn, creates a private cause of action. It states that "[a]ny person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court."

But what constitutes a "violation of this section"? Google claims that the Act is violated only when a video tape service provider discloses personally identifiable information, as proscribed in subsection (b). The plaintiffs, by contrast, insist that they are just as "aggrieved" when a third party receives personally identifiable information as when a video tape service provider discloses it. In support of this argument, the plaintiffs rely exclusively on a somewhat dated case from a district court in our Circuit, *Dirkes v. Borough of Runnemede* (D.N.J. 1996). We find the plaintiffs' reliance on *Dirkes* unpersuasive.

Dirkes was a former police officer who was suspected of stealing pornographic videos from a citizen's apartment. The allegations led local prosecutors to indict Dirkes for committing misconduct and led the local police department to open disciplinary proceedings. Even though Dirkes was eventually acquitted of the misconduct charge, the Borough's inquiry continued. A Borough investigator learned from a video store clerk that Dirkes had rented several pornographic movies, and information about Dirkes' video rental history was included in an internal affairs memorandum. That memorandum "was distributed to the Borough's special counsel, who in turn distributed it in connection with Plaintiff Dirkes' disciplinary hearing and in a proceeding before the Superior Court of New Jersey, Camden County."

In response to the dissemination of information about his video rental history, Dirkes and his wife sued the investigator, the police department, and the Borough for violating the Video Privacy Protection Act.[111] The district court rejected the defendants' argument that, as non-disclosing parties, they could not be liable under the Act. Instead, it reasoned that Congress's broad remedial purposes in passing the statute would best be served by allowing plaintiffs to sue "those individuals who have come to possess (and who could disseminate) the private information."

No other court has interpreted the Act this way. As the Sixth Circuit explained in *Daniel v. Cantrell* (2004), the better view is that subsection (b) makes certain conduct—the disclosure of personally identifiable information by a video tape service provider—unlawful, and subsection (c) creates a cause of action against persons who engage in such conduct.

Because we conclude that only video tape service providers that disclose personally identifiable information can be liable under subsection (c) of the Act, and because Google is not alleged to have disclosed any such information here, we will affirm the District Court's dismissal of the claim against Google.

2. Whether Viacom Disclosed "Personally Identifiable Information"

Viacom also argues that it never disclosed "personally identifiable information" about children who viewed videos on its websites. As we shall see, what counts as personally identifiable information under the Act is not entirely clear.

The plaintiffs claim that Viacom disclosed to Google at least eleven pieces of information about children who browsed its websites. Three, in particular, are central to their claim under the Act. The first is a user's IP address, "a number assigned to each device that is connected to the Internet" that permits computer-specific online tracking. The second is a user's browser and operating system settings, which comprise a so-called "browser fingerprint." The plaintiffs claim that these profiles are so detailed that the odds of two people having the same browser fingerprint are 1 in 286,777. The third is a computing device's "unique device identifier."

What these pieces of information have in common is that they allegedly permit Google to track the same computer across time. So, for example, if someone with a Google account were to run a Google search from his or her computer, and then that person's child were to visit Nick.com and watch a video on that same computer, the plaintiffs claim that Google could "match" the data (based on IP address, browser fingerprint, or unique device identifier) to determine that the same computer was involved in both activities. In the plaintiffs' view, this means that Viacom, by permitting Google to use cookies on its website, effectively disclosed "information which identifies [a particular child] as having requested or obtained specific video materials or services from a video tape service provider," thereby violating the Act. The plaintiffs also claim that Viacom acted "knowingly," as the Act requires, because Viacom

[111] Another section of the Act, 18 U.S.C. § 2710(b)(2)(C), permits a video tape service provider to disclose information "to a law enforcement agency pursuant to a warrant . . . , a grand jury subpoena, or a court order." The video clerk in *Dirkes* simply provided the information to the investigating officer when asked.

permitted Google to host ads on its websites despite being "aware of Google's ubiquitous presence on the Internet and its tracking of users."

Viacom, by contrast, argues that static digital identifiers, such as IP addresses, do not qualify as personally identifiable information. It encourages us to interpret the Act against the backdrop of the problem it was meant to rectify—the disclosure of an actual person's video rental history. So, for example, Viacom points to the Senate Report, which states that "personally identifiable information is intended to be transaction-oriented," meaning that it "identifies a particular person as having engaged in a specific transaction with a video tape service provider." Viacom reads this passage to suggest that the Act's authors had brick-and-mortar transactions in mind when they crafted the law. In Viacom's view, the information described by the plaintiffs is not personally identifiable because it does not, by itself, identify a particular person. Rather, it is "coded information, used for decades to facilitate the operation of the Internet, that theoretically could be used by the recipient to identify the location of a connected computer"—not to unmask the identity of a person using that computer.

The parties' contrasting positions reflect a fundamental disagreement over what kinds of information are sufficiently "personally identifying" for their disclosure to trigger liability under the Video Privacy Protection Act. At one end of the spectrum, of course, is a person's actual name. Then there are pieces of information, such as a telephone number or a physical address, which may not by themselves identify a particular person but from which it would likely be possible to identify a person by consulting publicly available sources, such as a phone book or property records. Further down the spectrum are pieces of information, like social security numbers, which are associated with individual persons but might not be easily matched to such persons without consulting another entity, such as a credit reporting agency or government bureau.

The kind of information at issue here—static digital identifiers—falls even further down the spectrum. To an average person, an IP address or a digital code in a cookie file would likely be of little help in trying to identify an actual person. A great deal of copyright litigation, for example, involves illegal downloads of movies or music online. Such suits often begin with a complaint against a "John Doe" defendant based on an Internet user's IP address. Only later, after the plaintiff has connected the IP address to an actual person by means of a subpoena directed to an Internet service provider, is the complaint amended to reflect the defendant's name.

Numerous district courts have grappled with the question of whether the Video Privacy Protection Act applies to static digital identifiers. Most have followed the rule adopted in *In re Hulu Privacy Litigation* (N.D. Cal. 2014). The court there concluded that static digital identifiers that could, in theory, be combined with other information to identify a person do not count as "personally identifiable information" under the Act, at least by themselves.

The district courts have not, however, been unanimous. The plaintiffs direct us to *Yershov v. Gannett Satellite Information Network, Inc* (D. Mass. 2015). The plaintiff there downloaded *USA Today*'s free application onto his smartphone. He alleged that Gannett, which publishes *USA Today*, shared information about videos he watched on his phone with a third-party analytics company, Adobe Systems, Inc. The information did not include the plaintiff's name or address, but rather his cell phone identification number and his GPS coordinates at the time he viewed a particular video. Rejecting the approach taken in *Hulu*, *Yershov* concluded that any unique identifier—including a person's smartphone ID—is personally identifiable information. It recognized that, in asking it to reach this conclusion, the plaintiff was "attempt[ing] to place a square peg (modern electronic technology) into a round hole (a statute written in 1988 aimed principally at videotape rental services)." Even so, the court stated that the Act applied to the disclosure of static identifiers that could theoretically permit a company like Adobe Systems to identify an individual video watcher. The First Circuit recently affirmed that conclusion.

In our view, the proper meaning of the phrase "personally identifiable information" is not straightforward. As a textual matter, "[t]he precise scope" of such information "is difficult to discern from the face of the statute—whether read in isolation or in its broader statutory context."

We begin with principles of statutory interpretation. Our review of the legislative history convinces us that Congress's purpose in passing the Video Privacy Protection Act was quite narrow: to prevent disclosures of information that would, with little or no extra effort, permit an ordinary recipient to identify a particular person's video-watching habits. We do not think that, when Congress passed the Act, it intended for the law to cover factual circumstances far removed from those that motivated its passage.

This becomes apparent by tracing the Video Privacy Protection Act's legislative history. The Senate version of the Act was introduced in May of 1988, and the coordinate House bill was introduced about a month later. The two bills were considered in a joint hearing in August of 1988 before the relevant House and Senate subcommittees. The then-extant Senate bill would have punished *both* disclosures relating to video tape service providers *and* disclosures relating to library borrowing records. Senator Patrick Leahy, Chairman of the Senate Subcommittee on Technology and the Law, characterized the purpose of the Senate bill as follows:

> Most of us rent movies at video stores and we check out books from our community libraries. These activities generate an enormous report of personal activity that, if it is going to be disclosed, makes it very, very difficult for a person to protect his or her privacy.
>
> It really isn't anybody's business what books or what videos somebody gets. It doesn't make any difference if somebody is up for confirmation as a Supreme Court Justice or they are running the local grocery store. It is not your business.

According to the Senate Report, the provisions of the Act relating to libraries were removed because the Senate Judiciary Committee "was unable to resolve questions regarding the application of such a provision for law enforcement." Even so, we think that legislators' initial focus on both libraries and video stores indicates that the Act was meant to prevent disclosures of information capable of identifying an *actual person's* reading or video-watching habits. We therefore agree with our colleagues who have reviewed this same legislative history and concluded that the Act "protects personally identifiable information that identifies a specific person and ties that person to particular videos that the person watched."

The plaintiffs contend that, contrary to our interpretation, Congress intended to pass a broad statute that would protect consumer privacy even as video-watching technology changed over time. To be fair, there are portions of the legislative history that might be read to support such a view. The text itself is also amenable to such an interpretation. After all, the Act says that personally identifiable information "*includes* information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider," and Congress's use of the word "includes" could suggest that Congress intended for future courts to read contemporary norms about privacy into the statute's original text. But we ultimately do not think that the definition of personally identifiable information in the Act is so broad as to cover the kinds of static digital identifiers at issue here. This is not to say that the Act has become a dead letter with the demise of the corner video store. If, for example, Google were to start purposefully leaking its customers' YouTube video-watching histories, we think such disclosures would almost certainly violate the Act. But trying to analogize between that kind of disclosure and Google's use of cookies on Viacom's websites is, at best, a strained enterprise.

Subsequent developments confirm this view. Congress amended the Video Privacy Protection in 2013, modifying those provisions of the law governing how a consumer can consent to the disclosure of personally identifiable information. The legislative history of the 2013

amendments demonstrates that Congress was keenly aware of how technological changes have affected the original Act. As one Senate report put it:

> At the time of the [1988 law's] enactment, consumers rented movies from video stores. The method that Americans used to watch videos in 1988—the VHS cassette tape—is now obsolete. In its place, the Internet has revolutionized the way that American consumers rent and watch movies and television programs. Today, so-called "on-demand" cable services and Internet streaming services allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones.

Despite this recognition, Congress did not update the definition of personally identifiable information in the statute. What's more, it chose not to do so despite the fact that the *amicus* supporting the plaintiffs here, the Electronic Privacy Information Center, submitted written testimony that included the following exhortation:

> [T]he Act does not explicitly include Internet Protocol (IP) Addresses in the definition [of personally identifiable information]. IP addresses can be used to identify users and link consumers to digital video rentals. They are akin to Internet versions of consumers' home telephone numbers. We would propose the addition of Internet Protocol (IP) Addresses and account identifiers to the definition of [personally identifiable information] . . . .

We think Congress's decision to retain the 1988 definition of personally identifiable information indicates that the Act serves different purposes, and protects different constituencies, than other, broader privacy laws.

Nor does our decision today create a split with our colleagues in the First Circuit. [T]he First Circuit focused on the fact that the defendant there allegedly disclosed not only what videos a person watched on his or her smartphone, but also the GPS coordinates of the phone's location at the time the videos were watched. In the First Circuit's view, "[g]iven how easy it is to locate a GPS coordinate on a street map, this disclosure would enable most people to identify what are likely the home and work addresses of the viewer (*e.g.*, Judge Bork's home and the federal courthouse)." That conclusion merely demonstrates that GPS coordinates contain more power to identify a *specific person* than, in our view, an IP address, a device identifier, or a browser fingerprint.

Of course, what we have said so far addresses the question of what counts as personally identifiable information in the abstract. The wrinkle in this case is that the party to whom the plaintiffs' information was disclosed is Google, a company whose entire business model is purportedly driven by the aggregation of information about Internet users. The plaintiffs assert that Google can identify web users in the real world, and indeed seem to believe that Google, which purportedly "knows more details about American consumers than any company in history," aggregates so much information that it has, in effect, turned the Internet into its own private data collection machine.

Whether or not this is true, we do not think that a law from 1988 can be fairly read to incorporate such a contemporary understanding of Internet privacy. The allegation that Google will assemble otherwise anonymous pieces of data to unmask the identity of individual children is, at least with respect to the kind of identifiers at issue here, simply too hypothetical to support liability under the Video Privacy Protection Act.

B. Intrusion upon Seclusion

Lastly, we turn to the plaintiffs' claim that Viacom and Google unlawfully invaded their privacy. The New Jersey Supreme Court, looking to the Second Restatement of Torts, has said that intrusion upon seclusion occurs whenever a plaintiff can show (i) an intentional intrusion

(ii) upon the seclusion of another that is (iii) highly offensive to a reasonable person. At least with respect to Viacom, we conclude that the plaintiffs have adequately alleged each of these three elements.

First, the plaintiffs have successfully alleged an "intentional intrusion." We considered this issue in *O'Donnell v. United States* (3d Cir. 1989), where we stated that "an actor commits an *intentional* intrusion only if he believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act." The defendants contend that *O'Donnell* bars the present claim because, after all, they installed cookies on the plaintiffs' computers under the belief that doing so was perfectly legal.

Indeed, *O'Donnell* itself focused on whether the alleged intrusion occurred without "legal *or* personal permission." Courts applying *O'Donnell* have appropriately treated the presence or absence of consent as a key factor in making this assessment. Whatever else the plaintiffs allege, they clearly assert that the defendants tracked their online behavior without their permission to do so.

Second, the plaintiffs have adequately alleged that the defendants invaded their privacy. We have embraced the Second Restatement's view that liability for intrusion only arises "when [the defendant] has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs." We think that a reasonable factfinder could conclude that Viacom's promise not to collect "ANY personal information" from children *itself* created an expectation of privacy with respect to browsing activity on the Nickelodeon website.

Third, the plaintiffs have adequately alleged, at least with respect to Viacom, that the intrusion on their privacy was "highly offensive to the ordinary reasonable man." The defendants disagree, contending that the use of cookies for benign commercial purposes has become so widely accepted a part of Internet commerce that it cannot possibly be considered "highly offensive." They also assert that the intrusion tort is more appropriately reserved for punishing behavior that is so offensive as to inspire out-and-out revulsion, as opposed to policing online business practices.

With respect to Google, we agree with the District Court. As Google fairly points out, courts have long understood that tracking cookies can serve legitimate commercial purposes. The plaintiffs do not challenge the proposition that the use of "cookies on websites geared toward adults" is generally acceptable, instead falling back on the claim that the use of cookies to track *children* is particularly odious. We are not so sure. Google used third-party cookies on Nick.com in the same way that it deploys cookies on myriad others websites. Its decision to do so here does not strike us as sufficiently offensive, standing alone, to survive a motion to dismiss.

As to Viacom, however, our conclusion is different. In the same way that Viacom's message to parents about not collecting children's personal information may have created an expectation of privacy on Viacom's websites, it also may have encouraged parents to permit their children to browse those websites under false pretenses. We recognize that some cases suggest that a violation of a technology company's privacy-related terms of service is not offensive enough to make out a claim for invasion of privacy. Even so, our decision in *Google* compels us to reach a different result. Just as *Google* concluded that a company may commit intrusion upon seclusion by collecting information using duplicitous tactics, we think that a reasonable jury could reach a similar conclusion with respect to Viacom.

Notes

1. Isn't this case just wrong? Disclosing to Google one's browser fingerprint and device identifier is, absent an unusual level of precaution, as good as disclosing one's name. Further, do you agree with the court's reading of the legislative history, particularly its

conclusion that a disclosure only counts if it permits identification with little to no extra effort?

In *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482 (1st Cir. 2016), the First Circuit held that disclosing the device's GPS coordinates at the moment of viewing and a unique Android identifier—capable of tracking the user across platforms—constituted disclosure of "personally identifiable information" under the VPPA. Unlike the Third Circuit's focus on historical circumstances, the First Circuit relied on the statute's broad and abstract text. It stressed that Congress's use of the word "includes" signaled an intent to protect more data than the statute explicitly states, and the Senate Report confirms that statute covers a minimum and non-exclusive set. The court further reasoned that GPS coordinates can readily identify an individual and, because Gannett knew the recipient could link the data to named users, that identification was reasonably foreseeable—contrary to *Nickelodeon's* conclusion that a static device ID is of little value to an average person. The Supreme Court has not yet addressed this apparent split.

2. In addition to companies that are obviously streaming service providers, some other actors have been held to be videotape service providers under the VPPA. For example, in *In re Vizio, Inc., Consumer Privacy Litigation* 238 F. Supp. 3d 1204, 1222 (C.D. Cal. 2017), TV manufacturer Vizio was held to be a videotape service provider because its collection of "Internet Apps and Internet Apps Plus are designed to enable consumers to seamlessly access Netflix, Hulu, YouTube, and Amazon Instant Video content in their homes." Further,

> Vizio then advertises its Smart TVs as "a passport to a world of entertainment, movies, TV shows and more," and charges consumers a premium for its Vizio Smart TVs specifically because these Smart TVs are designed to stream video content through Vizio's Internet Apps and Internet Apps Plus software. Essentially, Vizio has designed its Smart TVs to perform all the same functions of—and its Smart TVs are in direct competition with—Roku's devices; that Vizio has integrated what others sell as a separate device into its televisions makes no meaningful difference.

   The absence of any real videotapes was irrelevant because the statute's definition of "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials" can be compressed to "engaged in the business . . . of . . . delivery of . . . similar audio visual materials." And Vizio, in the eyes of the court, was in exactly that "business."[200]

3. Note the continued relevance of intrusion upon seclusion. Commentators sometimes argue that the privacy torts are irrelevant in this age of FTC enforcement and statutory causes of action. Yet the torts continue to crop up in the oddest places. They most often add value where, as here, the relevant statutory cause of action fails on a technical ground.

The final key term here is "consumer," defined as "any renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). This definition can be a challenge for plaintiffs. For instance, the Eleventh Circuit has held that "a person who downloads and uses a free mobile application on his smartphone to view freely available content, without more, is not a "subscriber" (and therefore not a "consumer") under the VPPA." *Ellis v. Cartoon Network, Inc.* 803 F.3d 1251, 1252 (11th Cir. 2015). Though monetary payment is not a strictly essential element, some amount of exchange and continued relationship is necessary to brand someone a subscriber, and thus consumer. *Yershov v. Gannett Satellite Information Network, Inc.* 820 F.3d 482, 487 (1st Cir. 2016). Obviously straightforward video

[200] The court noted that a mail carrier was not in that business because, though they might be delivering a tape, they were not "engaged in the business" of delivering tapes "because her job responsibilities are in no way tailored to delivering packages that contain videotapes as opposed to any other package."

purchase and rental, as in renting a video via Amazon, would be covered under the statute, as would subscribing to Netflix or Hulu.

Recently the 7th Circuit has adopted a broad definition of subscriber, holding that the exchange of valuable information for benefits is sufficient to make one a subscriber.

Gardner v. Me-TV National Limited Partnership, 132 F.4th 1022 (7th Cir. 2025)

Easterbrook, Circuit Judge.

When Robert Bork's nomination to the Supreme Court was defeated in 1987, his name became attached not only to a political strategy ("Borking") but also to a statute, 18 U.S.C. § 2710 (the "Bork Act"). This law, more formally called the Video Privacy Protection Act (VPPA or "the Act"), was the result of bipartisan revulsion against the ease with which reporters discovered what Bork and his family had rented on video tapes. The reporters did not turn up any dirt (Bork and his family watched Hitchcock mysteries, John Hughes comedies, British costume dramas, and spy thrillers) but the ready availability of rental information caused consternation in Congress, some members of which may have had other viewing predilections.

Using terminology that is now obsolete, the Act forbids the disclosure, by any "video tape service provider", of "personally identifiable information concerning any consumer of such provider" without the consumer's consent. 18 U.S.C. § 2710(b)(1). Section 2710(a)(4) defines "video tape service provider" to include any entity that sells, rents, or delivers "prerecorded video cassette tapes or similar audio visual materials"; the "similar" clause and the reference to "delivery" as well as rental makes the statute relevant to video that is streamed over the Internet. Under § 2710(a)(1) "the term 'consumer' means any renter, purchaser, or subscriber of goods or services from a video tape service provider". This suit presents the question what it means for a person to be a "subscriber", a term that the Act does not define.

MeTV operates a web site <https://www.metv.com> at which people can watch classic video programming—principally TV shows from the 1930s through the 1990s. Anyone can watch without providing personal information—though the site does need the viewer's Internet Protocol address, which is essential to deliver the video. A web browser supplies the IP address automatically. MeTV invites people to sign up in order to personalize their experience. In exchange for a person's email address and zip code (plus a self-selected user name and password), MeTV lets a person select TV shows to follow, receive reminders about when they come on (like an over-the-air station, MeTV shows programs on a schedule rather than on demand), use a "channel" finder feature, post comments about the programming, and receive notices about newly available programs.

MeTV does not charge the viewers; like over-the-air TV it makes money by selling ads. If someone just watches on the web site, advertisers cannot do much to target their pitches by viewers' (likely) preferences. The more person-specific information MeTV and its advertisers possess, the more closely they can target ads—and targeted ads sell for more than others. An email address and zip code help with targeting. And MeTV benefits when it can link a viewer to a Facebook account. Facebook collects lots of information that is available to someone who knows the user's Facebook identification number (FID). That number can be derived when someone already signed into Facebook uses the same browser to access MeTV. Plaintiffs allege that MeTV embeds in the videos a "Meta pixel" (named after the business that operates Facebook) that facilitates this linking. According to the complaint this lets Facebook know what the person is watching so it too can sell ads targeted to video preferences, and it improves MeTV's ability to promote its business on Facebook.

Plaintiffs allege in this case that they have "signed up" for MeTV, providing their email addresses and zip codes, and that they watch programming over MeTV while signed into Facebook in the same browser. This enables linking of accounts and better (from advertisers'

perspective) targeting of ads on both MeTV and Facebook. The complaint asserts that neither Facebook nor MeTV has plaintiffs' consent to provide the information in the Meta pixel. Section 2710(c) provides that persons injured by the un-consented disclosure of personally identifiable information may collect damages and attorneys' fees.

MeTV moved to dismiss the complaint, Fed. R. Civ. P. 12(b)(6), contending that plaintiffs are not "consumers" covered by the Act.

Here again is the definition of "consumer" in § 2710(a)(1): "any renter, purchaser, or subscriber of goods or services from a video tape service provider". Plaintiffs do not claim to be renters or purchasers, but they describe themselves as subscribers.

One possible response by MeTV would be that a "subscription" is something that costs money. A person who subscribes to Netflix pays a monthly fee. Someone who subscribes to the New York Times likewise pays a periodic fee to receive paper copies or to access news behind a paywall on the Internet. We assume that, as a matter of common usage, a "subscriber" gives value in exchange for goods or services. But MeTV does not contend that money is the *only* way to give value. In an Information Age, data can be worth more than money. If paying $1 a year to use MeTV would produce a subscription, then providing $1 worth of information must do so too. Every court of appeals that has considered the Act has reached this conclusion. See *Salazar v. National Basketball Association*, 118 F.4th 533, 550–53 (2d Cir. 2024); *Yershov v. Gannett Satellite Information Network, Inc.*, 820 F.3d 482, 487–89 (1st Cir. 2016); *Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251, 1255–57 (11th Cir. 2015). Cf. *Perry v. Cable News Network, Inc.*, 854 F.3d 1336, 1341–44 (11th Cir. 2017).

What MeTV argues instead is that plaintiffs subscribed to an *information* service (TV schedules and newsletters), not to a *video* service. Anyone can watch videos on the web site without supplying information (other than an IP address). This fact puts plaintiffs outside the statutory definition of "consumer", MeTV contends. And this is what the district court held.

Back to the definition of "consumer", for a third time: "any renter, purchaser, or subscriber of goods or services from a video tape service provider". This does not say "subscriber of ... *video* services"; it says "subscriber of ... services *from a video tape service provider*". The complaint adequately alleges that MeTV is a video tape service provider. What more is required? If plaintiffs had signed up and never watched a video, but had purchased a Flintstones sweatshirt or a Scooby Doo coffee mug or a Superman action figure or a Bugs Bunny puzzle (MeTV's web site offers all four), then they would have purchased "goods" from a "video tape service provider". Nothing in the Act says that the goods or services must be video tapes or streams.

The Act is aimed principally at information about videos; public disclosure of his rentals is what happened to Judge Bork. And what happened to Judge Bork has some overlap with what plaintiffs allege; after all, the Meta pixel encodes the name of each video that they stream from the website. But as far as the statute is concerned, this connection lies in the definition of "video tape service provider" rather than the definition of "consumer". Any purchase or subscription from a "video tape service provider" satisfies the definition of "consumer", even if the thing purchased is clothing or the thing subscribed to is a newsletter.

Our case is almost identical to *Salazar*. The decisions from the First Circuit and Eleventh Circuit (*Ellis, Yershov*, and *Perry*) ask whether a person becomes a "subscriber" by downloading and using an application ("app") that offers videos, without necessarily providing the app's creator with personal information such as a name or email address. The First Circuit and Eleventh Circuit have reached incompatible conclusions about how the definition in § 2710(a)(1) works for that situation. We do not address it here. It is enough to hold that, when a person does furnish valuable data in exchange for benefits, that person becomes a "consumer" as long as the entity on the other side of the transaction is a "video tape service provider". Plaintiffs' complaint survives a motion to dismiss under Rule 12(b)(6).

Notes

1. Is Easterbrook's appeal to textualism persuasive here? A week later the 6th Circuit disagreed in one respect, holding that a subscriber to a newsletter offered by a video tape service provider was not a consumer within the meaning of the VPPA. Though he subscribed to a product or service of a "video tape service provider," that product or service in question was not a "video cassette tape or similar audio visual material." *Salazar v. Paramount Glob.*, 133 F.4th 642, 653 (6th Cir. 2025). The Supreme Court has granted certiorari to Salazar and is likely to address this circuit split in its October 2026 term.
2. Easterbrook mentions a split between the 1st and 11th Circuits on the meaning of subscriber. Both circuits have faced cases in which a person has downloaded an application, not created an account, and watched video content. In *Yershov v. Gannett Satellite Information Network, Inc.*, 820 F.3d 482, 487–89 (1st Cir. 2016), the 1st Circuit held that this was sufficient to make someone a subscriber despite the lack of payment for the application. The 11th Circuit disagreed in *Perry v. Cable News Network, Inc.*, 854 F.3d 1336, 1341–44 (11th Cir. 2017), holding that the plaintiff needed to show some sort of "ongoing commitment or relationship between the user and the entity which owns and operates the app," for example a registered account.
3. Many defense-side firms are greatly concerned by the broad scope granted to the VPPA under recent decisions. They note that these suits may be driven by the attractiveness of the VPPA's statutory remedies, which permit "any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court."

> (2) The court may award—
>
> > (A) actual damages but not less than liquidated damages in an amount of $2,500;
> > (B) punitive damages;
> > (C) reasonable attorneys' fees and other litigation costs reasonably incurred; and
> > (D) such other preliminary and equitable relief as the court determines to be appropriate.

E. Biometric Privacy

Issues of biometric privacy have arisen with increasing frequency over the last decade as biometric scanners have become cheaper and more prevalent.[201] Many employers make their employees clock into and out of work using fingerprints rather than timecards. Banks and other financial institutions use biometrics of all sorts for an extra level of security, and now so do some educational testing centers. Airlines use facial recognition to verify passenger identities at check-in. Retail stores use facial recognition to track suspected shoplifters, and some companies are reportedly using it to track all shoppers in their stores. Along with this increased use has come a wave of litigation against technology companies that use facial recognition to identify people in photographs and employers that use fingerprint biometric scanners for employee timekeeping.[202]

In addition to this private sector activity, governments at all levels have begun to experiment with facial recognition, particularly in law enforcement, though uses are generally

---

[201] Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 435–37 (2018) (reviewing the increased use of biometrics across industries).

[202] *See generally* Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms,* 10 U.C. IRVINE L. REV. 107 (2019).

limited thus far.[203] Overseas, biometric usage has already been taken to the next level. The Chinese government, for instance, has deployed facial recognition systems to identify people at public events who are suspected of minor crimes, and it is also using facial recognition to identify jaywalkers and red-light runners.

Despite its increasing importance and use, there is limited regulation of biometric identification. The primary law used to this point is Illinois' Biometric Information Privacy Act (BIPA). This sleeper statute was passed in 2008 and largely ignored until the mid-2010s. By 2020, however, hundreds of BIPA lawsuits had been filed. Though other states have biometric privacy statutes, only BIPA has yet spawned this wave of litigation. It is therefore an instructive example of how the procedural aspects of a privacy statute inform its substantive effects. The other major statutes are that of Texas—enforceable only by the state attorney general, and thus the grounds for very few lawsuits as yet—and the newly passed My Health My Data Act in Washington State (covered in Chapter 7). Most states do not have standalone biometric privacy statutes, and their broader consumer privacy and data breach statutes are mostly untested as they relate to biometric privacy.

Most biometrics are used in the same two ways: they either identify or authenticate an individual. Upon enrollment in a biometric system, a person's biometric identifier is scanned and converted into a digital code. When that person's biometric is later scanned again, the results of the second scan can be compared to those of the earlier scan to determine whether there is a match. This can be done to either confirm the identity of an individual—"Is this Jane, the owner of the account?"—or to identify an unknown person by comparing the novel digital code to a database of potential matches. To serve this purpose, biometrics identification must be based on some unique physiological characteristic that is naturally stable and hard to artificially alter. Weight is a poor biometric for identification because it fluctuates hourly and daily and is common across many people. Iris recognition is a great biometric because it is highly stable and unique.

In the context of facial recognition, biometric privacy is hugely important. Faces are widely shown to the public at large, and thus facial biometrics can be captured and compared at a distance and without consent. Facial recognition can turn every stadium, shopping mall, and city street in America into a dystopian surveillance state, with every venue or shop owner able to identify and track all those who pass by. Fingerprint biometrics offer fewer obvious problems—fingerprints do not so readily allow for public tracking. More novel forms of biometrics—such as gait, finger-swipe, and keystroke pattern recognition—are also distinct use cases, with both pluses and minuses from a privacy perspective.

Biometric privacy statutes have, in general, not sought to draw distinctions between fingerprints, voiceprints, and facial recognition information. BIPA, for instance, defines biometric identifier as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color." BIPA does not consider swipe or gait biometrics because they were not major identifiers when the statute was passed.

Having defined biometrics thusly, BIPA then protects them by prohibiting private entities from collecting, purchasing, receiving through trade, or otherwise obtaining biometrics without the written consent of the data subject. Further, the data subject must receive a series of specific disclosures in writing (such as the length of time the information would be retained and how it would be used). The biometric can *never* be sold, leased, traded, or otherwise profited

[203] *See generally* Matthew B. Kugler, *Public Perceptions Can Guide Regulation of Public Facial Recognition*, 25 COLUM. SCI. & TECH. L. REV. 1 (2023).

from, and the biometric cannot be disclosed without the consent of the data subject or as required by law. The biometric also must be stored securely.

The very simplicity of this statute makes it immensely powerful. For the first few years of litigation, however, it was unclear whether technical violations of the statute's notice and consent provisions were independently actionable. The below case settled that question and is often credited with turning the initial flood of BIPA lawsuits into a flood of plaintiff-friendly settlements.

Rosenbach v. Six Flags Entertainment Corporation, 129 N.E.3d 1197 (Ill. 2019)

CHIEF JUSTICE KARMEIER delivered the judgment of the court, with opinion.

The Biometric Information Privacy Act (740 ILCS 14/1) imposes numerous restrictions on how private entities collect, retain, disclose and destroy biometric identifiers, including retina or iris scans, fingerprints, voiceprints, scans of hand or face geometry, or biometric information. Under the Act, any person "aggrieved" by a violation of its provisions "shall have a right of action . . . against an offending party" and "may recover for each violation" the greater of liquidated damages or actual damages, reasonable attorney fees and costs, and any other relief, including an injunction, that the court deems appropriate. The central issue in this case . . . is whether one qualifies as an "aggrieved" person and may seek liquidated damages and injunctive relief pursuant to the Act if he or she has not alleged some actual injury or adverse effect, beyond violation of his or her rights under the statute.

Six Flags Entertainment Corporation and its subsidiary Great America LLC own and operate the Six Flags Great America amusement park in Gurnee, Illinois. Defendants sell repeat-entry passes to the park. Since at least 2014, defendants have used a fingerprinting process when issuing those passes. As alleged by the complaint, their system "scans pass holders' fingerprints; collects, records and stores 'biometric' identifiers and information gleaned from the fingerprints; and then stores that data in order to quickly verify customer identities upon subsequent visits by having customers scan their fingerprints to enter the theme park." According to the complaint, "[t]his makes entry into the park faster and more seamless, maximizes the time pass holders are in the park spending money, and eliminates lost revenue due to fraud or park entry with someone else's pass."

In May or June 2014, while the fingerprinting system was in operation, Stacy Rosenbach's 14-year-old son, Alexander, visited defendants' amusement park on a school field trip. In anticipation of that visit, Rosenbach had purchased a season pass for him online. Rosenbach paid for the pass and provided personal information about Alexander, but he had to complete the sign-up process in person once he arrived at the amusement park.

The process involved two steps. First, Alexander went to a security checkpoint, where he was asked to scan his thumb into defendants' biometric data capture system. After that, he was directed to a nearby administrative building, where he obtained a season pass card. The card and his thumbprint, when used together, enabled him to gain access as a season pass holder.

Upon returning home from defendants' amusement park, Alexander was asked by Rosenbach for the booklet or paperwork he had been given in connection with his new season pass. In response, Alexander advised her that defendants did "it all by fingerprint now" and that no paperwork had been provided.

The complaint alleges that this was the first time Rosenbach learned that Alexander's fingerprints were used as part of defendants' season pass system. Neither Alexander, who was a minor, nor Rosenbach, his mother, were informed in writing or in any other way of the specific purpose and length of term for which his fingerprint had been collected. Neither of them signed

any written release regarding taking of the fingerprint, and neither of them consented in writing "to the collection, storage, use sale, lease, dissemination, disclosure, redisclosure, or trade of, or for [defendants] to otherwise profit from, Alexander's thumbprint or associated biometric identifiers or information."

The school field trip was Alexander's last visit to the amusement park. Although he has not returned there since, defendants have retained his biometric identifiers and information. They have not publicly disclosed what was done with the information or how long it will be kept, nor do they have any "written policy made available to the public that discloses [defendants'] retention schedule or guidelines for retaining and then permanently destroying biometric identifiers and biometric information."

In response to the foregoing events, Rosenbach, acting in her capacity as mother and next friend of Alexander, brought this action on his behalf in the circuit court of Lake County. The action seeks redress for Alexander, individually and on behalf of all other similarly situated persons . . . .

The Biometric Privacy Information Act . . . was enacted in 2008 to help regulate "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." The Act defines "biometric identifier" to mean "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." "Biometric information" means "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." It is undisputed that the thumbprint collected by defendants from Rosenbach's son, Alexander, when they processed his season pass constituted a biometric identifier subject to the Act's provisions and that the electronically stored version of his thumbprint constituted biometric information within the meaning of the law.

Section 15 of the Act imposes on private entities such as defendants' various obligations regarding the collection, retention, disclosure, and destruction of biometric identifiers and biometric information. Among these is the following:

> "(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> > (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
> >
> > (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
> >
> > (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

These provisions are enforceable through private rights of action. Specifically, section 20 of the Act provides that "[a]ny person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party." Section 20 further provides that

> "[a] prevailing party may recover for each violation:
>
> (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;

(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate."

As noted earlier in this opinion, Rosenbach's complaint alleges that defendants violated the provisions of section 15 of the Act when it collected her son's thumbprint without first following the statutorily prescribed protocol. The basis for defendants' current challenge is that no other type of injury or damage to Rosenbach's son has been alleged. Rosenbach seeks redress on her son's behalf and on behalf of a class of similarly situated individuals based solely on defendants' failure to comply with the statute's requirements.

We begin our analysis with basic principles of statutory construction. When construing a statute, our primary objective is to ascertain and give effect to the legislature's intent. That intent is best determined from the plain and ordinary meaning of the language used in the statute. When the statutory language is plain and unambiguous, we may not depart from the law's terms by reading into it exceptions, limitations, or conditions the legislature did not express, nor may we add provisions not found in the law.

Defendants read the Act as evincing an intention by the legislature to limit a plaintiff's right to bring a cause of action to circumstances where he or she has sustained some actual damage, beyond violation of the rights conferred by the statute, as the result of the defendant's conduct. This construction is untenable. When the General Assembly has wanted to impose such a requirement in other situations, it has made that intention clear. Section 10a(a) of the Consumer Fraud and Deceptive Business Practices Act (815 ILCS 505/10a(a)) is an example. To bring a private right of action under that law, actual damage to the plaintiff must be alleged.

In contrast is the AIDS Confidentiality Act (410 ILCS 305/1). There, the legislature authorized private rights of action for monetary relief, attorney fees, and such other relief as the court may deem appropriate, including an injunction, by any person "aggrieved" by a violation of the statute or a regulation promulgated under the statute. Proof of actual damages is not required in order to recover.

Section 20 of the Act, the provision that creates the private right of action on which Rosenbach's cause of action is premised, clearly follows the latter model. In terms that parallel the AIDS Confidentiality Act, it provides simply that "[a]ny person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party."

More than a century ago, our court held that to be aggrieved simply "means having a substantial grievance; a denial of some personal or property right." *Glos v. People* (Ill. 1913). A person who suffers actual damages as the result of the violation of his or her rights would meet this definition of course, but sustaining such damages is not necessary to qualify as "aggrieved." Rather, "[a] person is prejudiced or aggrieved, in the legal sense, when a legal right is invaded by the act complained of *or* his pecuniary interest is directly affected by the decree or judgment." (Emphasis added.)

The foregoing understanding of the term is also consistent with standard definitions of "aggrieved" found in dictionaries . . . . Merriam-Webster's Collegiate Dictionary, for example, defines aggrieved as "suffering from an infringement or denial of legal rights." Similarly, the leading definition given in Black's Law Dictionary is "having legal rights that are adversely affected." This is therefore the meaning we believe the legislature intended here.

In sum, defendants' contention that redress under the Act should be limited to those who can plead and prove that they sustained some actual injury or damage beyond infringement of the rights afforded them under the law would require that we disregard the commonly understood and accepted meaning of the term "aggrieved," depart from the plain and, we believe, unambiguous language of the law, read into the statute conditions or limitations the legislature did not express, and interpret the law in a way that is inconsistent with the objectives and purposes the legislature sought to achieve. That, of course, is something we may not and will not do.

Notes

1. *Rosenbach* initially appears to be a mundane statutory construction case. But consider the consequences. BIPA requires that a private entity obtain a *written* release after first informing the data subject in *writing* about a *series* of things. These requirements are not difficult to satisfy in many cases *if one seeks to satisfy them*. An employer, for instance, could easily have their lawyers write a BIPA-complaint consent form and have everyone sign it. But most employers had not sought to do this. And, due to the specificity required under BIPA, companies would not have complied with it by accident—consider that the entity must state both the specific purpose for which the biometric is being collected and also provide a retention schedule. *Rosenbach* holds that such paperwork failures are sufficient to bring a BIPA claim even absent any further proof of harm.
2. BIPA has substantial statutory damages. Rather than the Rosenbach's needing to quantify the privacy or dignitary cost of not having their consent appropriately obtained, they can instead ask for what the statute provides: $1,000 for negligent violations and $5,000 for intentional or reckless violations. This leads to the horrifying math of BIPA: a company with 200 employees and a fingerprint scanner might easily be out $200,000. Facebook, with millions of Illinois users, was contemplating billions in potential liability before settling for a mere $650 million. Six Flags ultimately settled for $36 million.
3. Though employers can easily comply with BIPA's consent and data security requirements if they plan ahead, other uses are simply impossible. Clearview AI's web crawlers sought to make use all photos uploaded to the internet for facial recognition. That cannot be done with the photos of Illinois users without their consent, and their consent cannot reasonably be obtained. Video doorbells often use facial recognition to identify visitors. Major vendors have turned that feature off in Illinois; consent cannot reliably be obtained from all who would approach a door.
4. On legislative sausage-making: BIPA was passed by the Illinois legislature rather than by the U.S. Congress. The available legislative history of BIPA is effectively nonexistent; my article on BIPA reviews the existing legislative materials in about a page and a half. Based on the limited available documents and interviews with several involved parties, it appears that BIPA was largely the brainchild of James Ferg-Cadima, then of the ACLU. The bill received some initial pushback from industries that did not wish to be regulated by it: government actors, banks, and medical professionals. After amendments, BIPA does not apply to government actors, banks, and "information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996." The congruence between exemptions and lobbyist involvement is not coincidental.
5. In *Mosby v. Ingalls Memorial Hospital* 2023 IL 129081 (2023), the Illinois Supreme Court held that the medical exemption under BIPA allowed hospitals to use biometrics to control employee access to medications even without employee consent. It read the "or" in the preceding note to mean that "information collected, used or stored for healthcare treatment, payment, or operations" was independently exempt from BIPA's coverage even if it was not patient data.
6. BIPA applies only to private actors, meaning the government is left unregulated. In general, there are few laws, anywhere in the country, preventing government use of biometric

information. Though some municipalities have banned facial recognition, these are very few in number and make up a vanishingly small proportion of the cities and towns in the United States. And, though some have argued that government use of facial recognition is a Fourth Amendment search,[204] this argument has yet to be accepted by courts.

7. One thing often lost in discussions of biometrics is the heterogeneity of the uses of biometric technology. In an empirical article published in 2019, I showed that people have sharply different comfort levels with different use cases.[205] Notable (to me) is the sharp divide between high comfort with the use of biometric technology by a store to detect known shoplifters and the lower comfort with the same store (the descriptions were identical) using the same technology to better target advertising. In general, however, public tracking uses elicit much lower comfort ratings than the life-convenience uses.

	Comfort (1-6)		Comfort Below Mid-point	Comfort Above Mid-point
Fingerprint to unlock bank's smartphone app	4.03	(1.73)	35.0%	65.0%
Voiceprint to confirm identity when calling CC company	3.64	(1.74)	45.3%	54.7%
Smart doorbell with facial recognition to identify visitors	3.99	(1.69)	36.1%	63.9%
Fingerprint to open locker holding package	3.89	(1.68)	38.3%	61.7%
Performance venue facial recognition to ID known stalkers	3.84	(1.70)	40.0%	60.0%
Facial recognition to unlock smartphone	3.85	(1.73)	41.1%	58.9%
Fingerprint to unlock smartphone	4.29	(1.65)	28.9%	71.1%
Store using facial recognition to detect known shoplifters	3.77	(1.76)	41.1%	58.9%
Store using facial recognition to track shoppers around store and serve targeted ads	2.49	(1.65)	74.2%	25.8%
Company using facial recognition to comb social media to track photos/locations of celebrities	2.52	(1.61)	73.8%	26.2%
Company using facial recognition to link profiles across social media sites	2.71	(1.69)	69.1%	30.9%
Company using facial recognition to identify unknown persons in uploaded photos.	3.20	(1.70)	57.0%	43.0%
Company using facial recognition to track people's locations using publicly uploaded photos.	2.59	(1.66)	71.3%	28.7%
A homeowner's association using facial recognition to track the movements of people on its streets and sidewalks.	2.71	(1.72)	68.1%	31.9%
Company using facial recognition to find photos of its users on other companies' websites.	2.77	(1.67)	67.2%	32.8%
An employer using fingerprint scans rather than timecards for people to check in at work.	3.96	(1.74)	37.4%	62.6%
A coffee shop using facial recognition rather than id cards to administer their customer loyalty program, with cameras identifying people as they approach the counter.	2.89	(1.69)	64.8%	35.2%
A gym having their members check-in using a fingerprint scan rather than an id card.	3.80	(1.75)	41.2%	58.8%

Note: The comfort rating column gives mean and standard deviations for each type of search. "CC company" means "credit card company."

8. Another survey asked participants—who had been instructed to consider either facial or fingerprint recognition in the context of basic consumer transactions—why they did, or did not, feel comfortable with companies collecting their biometric information. Notable here is

[204] *See, e.g.*, Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105 (2021).

[205] Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms,* 10 U.C. IRVINE L. REV. 108 (2019).

the wide range of reasons selected by participants who were uncomfortable (they were all allowed to select multiple options).

Reasons for Discomfort	Facial Geometry	Fingerprint
It feels very invasive for a company to collect and share [this] information.	69.70%	71.00%
I'm worried about where the collection of [this] information might lead in the future.[1]	67.30%	66.00%
[This] information could be used to track me in public, and I don't want companies having that power.	62.70%	55.40%
A company having [this] information makes it more likely that my identity could be stolen.	52.80%	57.50%
[This] information could be used to find out other things about me.	41.00%	46.40%
[This] information is a part of me.	30.70%	32.80%
[This] information is something I can't change.	22.20%	28.40%
Other (please explain)	3.30%	3.40%

Reasons for Comfort	Facial Geometry	Fingerprint
I have nothing to hide that [this] information would reveal.	49.50%	57.40%
Companies having [this] information could use it make my life easier in some way.	31.50%	30.80%
[This] information is already so public that it doesn't matter if another company has it.	27.70%	31.70%
I don't see how [this] information could be misused or abused.	24.10%	19.20%
I have a credit monitoring/identity monitoring service, so I am covered even if [this] information is abused.	19.30%	17.90%
Other (please explain)	3.50%	1.90%

The issue of varying uses of biometric data is clearly presented in the below case against Facebook, which concerned facial recognition data.

Patel v. Facebook 932 F.3d 1264 (9th Cir. 2019)

IKUTA, Circuit Judge:

Plaintiffs' complaint alleges that Facebook subjected them to facial-recognition technology without complying with an Illinois statute intended to safeguard their privacy. Because a violation of the Illinois statute injures an individual's concrete right to privacy, we reject Facebook's claim that the plaintiffs have failed to allege a concrete injury-in-fact for purposes of Article III standing. Additionally, we conclude that the district court did not abuse its discretion in certifying the class.

I

Facebook operates one of the largest social media platforms in the world, with over one billion active users. About seven in ten adults in the United States use Facebook.

A

When a new user registers for a Facebook account, the user must create a profile and agree to Facebook's terms and conditions, which permit Facebook to collect and use data in accordance with Facebook's policies. To interact with other users on the platform, a Facebook user identifies another user as a friend and sends a friend request. If the request is accepted, the two users are able to share content, such as text and photographs.

For years, Facebook has allowed users to tag their Facebook friends in photos posted to Facebook. A tag identifies the friend in the photo by name and includes a link to that friend's Facebook profile. Users who are tagged are notified of the tag, granted access to the photo, and allowed to share the photo with other friends or "un-tag" themselves if they choose.

In 2010, Facebook launched a feature called Tag Suggestions. If Tag Suggestions is enabled, Facebook may use facial-recognition technology to analyze whether the user's Facebook friends are in photos uploaded by that user. When a photo is uploaded, the technology scans the photo and detects whether it contains images of faces. If so, the technology extracts the various geometric data points that make a face unique, such as the distance between the eyes, nose, and ears, to create a face signature or map. The technology then compares the face signature to faces in Facebook's database of user face templates (i.e., face signatures that have already been matched to the user's profiles).[2] If there is a match between the face signature and the face template, Facebook may suggest tagging the person in the photo.

Facebook's face templates are stored on its servers, which are located in nine data centers maintained by Facebook. The six data centers located in the United States are in Oregon, California, Iowa, Texas, Virginia, and North Carolina. Facebook's headquarters are in California.

B

Facebook users living in Illinois brought a class action against Facebook, claiming that Facebook's facial-recognition technology violates Illinois law. Class representatives Adam Pezen, Carlo Licata, and Nimesh Patel each live in Illinois. They joined Facebook in 2005, 2009, and 2008, respectively, and each uploaded photos to Facebook while in Illinois. Facebook created and stored face templates for each of the plaintiffs.

The three named plaintiffs filed the operative consolidated complaint in a California district court in August 2015. The plaintiffs allege that Facebook violated the Illinois Biometric Information Privacy Act (BIPA), which provides that "[a]ny person aggrieved" by a violation of its provisions "shall have a right of action" against an "offending party." According to the complaint, Facebook violated sections 15(a) and 15(b) of BIPA by collecting, using, and storing biometric identifiers (a "scan" of "face geometry") from their photos without obtaining a written release and without establishing a compliant retention schedule.

The Illinois General Assembly enacted BIPA in 2008 to enhance Illinois's "limited State law regulating the collection, use, safeguarding, and storage of biometrics." To further these goals, section 15 of BIPA imposes "various obligations regarding the collection, retention, disclosure, and destruction of biometric identifiers and biometric information" on private entities. *Rosenbach v. Six Flags Entm't Corp.* (Ill. 2019). These requirements include "establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information" the earlier of three years after the individual's last interaction with the private entity or "when the initial purpose for collecting or obtaining such identifiers or information has been satisfied." The statute also requires the private entity to notify the individual in writing and secure a written release before obtaining a biometric identifier. BIPA also provides for actual and liquidated damages for violations of the Act's requirements.

C

In June 2016, Facebook moved to dismiss the plaintiffs' complaint for lack of Article III standing on the ground that the plaintiffs had not alleged any concrete injury.

---

[2] According to Facebook, it creates and stores a template for a user when the user (1) has been tagged in at least one photo; (2) has not opted out of Tag Suggestions; and (3) satisfies other privacy-based and regulatory criteria.

II

To establish Article III standing, a plaintiff "must have suffered an 'injury in fact'—an invasion of a legally protected interest which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical." A plaintiff does not necessarily meet the concrete injury requirement "whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." *Spokeo, Inc. v. Robins* 136 S. Ct. 1540, 1549 (2016) (*Spokeo I*). In other words, for Article III purposes, it is not enough for a plaintiff to allege that a defendant has violated a right created by a statute; we must still ascertain whether the plaintiff suffered a concrete injury-in-fact due to the violation.

A concrete injury need not be tangible. "Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete." In determining whether an intangible injury is sufficiently concrete, we consider both history and legislative judgment. We consider history because "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." We must also examine legislative judgment because legislatures are "well positioned to identify intangible harms that meet minimum Article III requirements."

The Supreme Court has provided some guidance for determining whether a plaintiff has suffered a concrete injury due to a defendant's failure to comply with a statutory requirement. The violation of a statutory right that protects against "the risk of real harm" may be sufficient to constitute injury-in-fact, and under those circumstances a plaintiff "need not allege any *additional* harm beyond the one Congress has identified." But a violation of a statutory procedural requirement that does not present a material risk of harm, such as dissemination of "an incorrect zip code," likely does not cause a concrete injury.

In light of this guidance, we have adopted a two-step approach to determine whether the violation of a statute causes a concrete injury. We ask "(1) whether the statutory provisions at issue were established to protect [the plaintiff's] concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests." *Robins v. Spokeo, Inc.* 867 F.3d 1108, 1113 (9th Cir. 2017) (*Spokeo II*).

Other cases demonstrate these principles. In *Van Patten v. Vertical Fitness Group, LLC* (9th Cir. 2017), for instance, we considered a Telephone Consumer Protection Act (TCPA) requirement prohibiting a telemarketer from calling or texting a consumer without the consumer's consent. The plaintiff alleged that a telemarketer violated this prohibition. We held that the TCPA was established to protect the plaintiff's substantive right to privacy, namely the right to be free from unsolicited telemarketing phone calls or text messages that "invade the privacy and disturb the solitude of their recipients." Because the telemarketer's conduct impacted this privacy right, we concluded that the plaintiff did not need to allege any additional harm beyond the one Congress identified, and therefore had alleged a concrete injury-in-fact sufficient to confer Article III standing.

By contrast, in *Bassett v. ABM Parking Services, Inc.* (9th Cir. 2018), we considered a Fair Credit Reporting Act (FCRA) requirement that businesses redact certain credit card information, including the card's expiration date, on printed receipts. The plaintiff alleged that a parking garage had violated this requirement by giving him a receipt displaying his card's full expiration date. We held that even if the FCRA created a substantive right to the "nondisclosure of a consumer's private financial information to identity thieves," the parking garage's failure to redact the credit card's expiration date did not impact this substantive right, because no one but the plaintiff himself saw the expiration date. We therefore concluded that the plaintiff had failed to allege a concrete injury-in-fact.

A

Facebook argues that the plaintiffs' complaint describes a bare procedural violation of BIPA rather than injury to a concrete interest, and therefore plaintiffs failed to allege that they suffered an injury-in-fact that is sufficiently concrete for purposes of standing. Plaintiffs, in turn, argue that Facebook's violation of statutory requirements amounted to a violation of their substantive privacy rights, and so they suffered a concrete injury for purposes of Article III standing.

In addressing these arguments, we first consider "whether the statutory provisions at issue were established to protect [the plaintiff's] concrete interests (as opposed to purely procedural rights)." *Dutta v. State Farm Mut. Auto. Ins. Co.* (9th Cir. 2018) (alteration in original) (quoting *Spokeo II*). Privacy rights have long been regarded "as providing a basis for a lawsuit in English or American courts." *Spokeo I*. The common law roots of the right to privacy were first articulated in the 1890s in an influential law review article that reviewed 150 years of privacy-related case law and identified "a general right to privacy" in various common law property and defamation actions. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

In its recent Fourth Amendment jurisprudence, the Supreme Court has recognized that advances in technology can increase the potential for unreasonable intrusions into personal privacy. These concerns extend to sense-enhancing thermal imaging, *see Kyllo v. United States* (2001); GPS monitoring for extended periods of time, *see United States v. Jones*, (2012) (Sotomayor, J., concurring, and Alito, J., concurring) (five justices agreeing that privacy concerns are raised by such monitoring, as later recognized in *Carpenter v. United States* (2018)); modern cell phone storage of "vast quantities of personal information," *Riley v. California* (2014); and technological advances in tracking cell-site location information, *see Carpenter*. Technological advances provide "access to a category of information otherwise unknowable," *Carpenter*, and "implicate privacy concerns" in a manner as different from traditional intrusions as "a ride on horseback" is different from "a flight to the moon," *Riley*.

In light of this historical background and the Supreme Court's views regarding enhanced technological intrusions on the right to privacy, we conclude that an invasion of an individual's biometric privacy rights "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Spokeo I*. As in the Fourth Amendment context, the facial-recognition technology at issue here can obtain information that is "detailed, encyclopedic, and effortlessly compiled," which would be almost impossible without such technology. *Carpenter*. Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual's Facebook friends or acquaintances who are present in the photo. Taking into account the future development of such technology as suggested in *Carpenter*, it seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual's cell phone. We conclude that the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests. Similar conduct is actionable at common law.

The judgment of the Illinois General Assembly, which is "instructive and important" to our standing inquiry, *Spokeo II* (quotation omitted), supports the conclusion that the capture and use of a person's biometric information invades concrete interests. As noted above, in enacting BIPA, the General Assembly found that the development and use of biometric data presented risks to Illinois's citizens, and that "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." Interpreting the statute, the Illinois

Supreme Court concluded that "[t]he strategy adopted by the General Assembly through enactment of [BIPA]" was to protect individuals' "biometric privacy" by (1) "imposing safeguards to insure that individuals' and customers' privacy rights in their biometric identifiers and biometric information are properly honored and protected to begin with, before they are or can be compromised," and (2) "by subjecting private entities who fail to follow the statute's requirements to substantial potential liability." *Rosenbach*. Based on this interpretation, the Illinois Supreme Court concluded that an individual could be "aggrieved" by a violation of BIPA whenever "a private entity fails to comply with one of section 15's requirements," because "that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach." Individuals are not required to sustain a "compensable injury beyond violation of their statutory rights before they may seek recourse."

Therefore, we conclude that "the statutory provisions at issue" in BIPA were established to protect an individual's "concrete interests" in privacy, not merely procedural rights. *Spokeo II*.

B

We next turn to the question "whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests." *Spokeo II*. Facebook's relevant conduct, according to the complaint, is the collection, use, and storage of biometric identifiers without a written release, in violation of section 15(b), and the failure to maintain a retention schedule or guidelines for destroying biometric identifiers, in violation of section 15(a). The plaintiffs allege that a violation of these requirements allows Facebook to create and use a face template and to retain this template for all time. Because the privacy right protected by BIPA is the right not to be subject to the collection and use of such biometric data, Facebook's alleged violation of these statutory requirements would necessarily violate the plaintiffs' substantive privacy interests. As the Illinois Supreme Court explained, the procedural protections in BIPA "are particularly crucial in our digital world" because "[w]hen a private entity fails to adhere to the statutory procedures . . . the right of the individual to maintain his or her biometric privacy vanishes into thin air." *Rosenbach*. Accordingly, we conclude that the plaintiffs have alleged a concrete injury-in-fact sufficient to confer Article III standing.

III

We now turn to Facebook's argument that the district court abused its discretion by certifying the class.

First, Facebook urges that class certification is not compatible with Rule 23(b)(3) of the Federal Rules of Civil Procedure, which requires that "questions of law or fact common to class members predominate over any questions affecting only individual members." According to Facebook, the Illinois extraterritoriality doctrine precludes the district court from finding predominance.

The Illinois Supreme Court has held that it is a "long-standing rule of construction in Illinois" that "a 'statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute.'" In the absence of such an intent, an Illinois plaintiff may not maintain a cause of action under a state statute for transactions that took place outside of Illinois. When a case is "made up of components that occur in more than one state," plaintiffs may maintain an action only if the events that are necessary elements of the transaction occurred "primarily and substantially within" Illinois.

Facebook insists that the Illinois legislature did not intend for the BIPA to have extraterritorial effect, and in the absence of such an intent, a court would have to consider whether the relevant events at issue took place inside or outside Illinois. Facebook argues that its collection of biometric data and creation of a face template occurred on its servers outside of

Illinois, and therefore the necessary elements of any violation occurred extraterritorially. At best, Facebook argues, each class member would have to provide individualized proof that events in that class member's case occurred "primarily and substantially within" Illinois; for instance, that the member was in Illinois when the scanned photo was taken or uploaded, when a facial recognition analysis was performed, when the photo was tagged or given a tag suggestion, or for similar events. Because the district court would have to conduct countless mini-trials to determine whether the events in each plaintiff's case occurred "primarily and substantially within" Illinois, Facebook posits, common questions do not predominate, and the district court erred in certifying the class.

We disagree. The parties' dispute regarding extraterritoriality requires a decision as to where the essential elements of a BIPA violation take place. The statute does not clarify whether a private entity's collection, use, and storage of face templates without first obtaining a release, or a private entity's failure to implement a compliant retention policy, is deemed to occur where the person whose privacy rights are impacted uses Facebook, where Facebook scans photographs and stores the face templates, or in some other place or combination of places. Given the General Assembly's finding that "[m]ajor national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions," it is reasonable to infer that the General Assembly contemplated BIPA's application to individuals who are located in Illinois, even if some relevant activities occur outside the state. These threshold questions of BIPA's applicability can be decided on a class-wide basis. If the violation of BIPA occurred when the plaintiffs used Facebook in Illinois, then the relevant events occurred "primarily and substantially" in Illinois, and there is no need to have mini-trials on this issue. If the violation of BIPA occurred when Facebook's servers created a face template, the district court can determine whether Illinois's extraterritoriality doctrine precludes the application of BIPA. In either case, predominance is not defeated. And of course, if future decisions or circumstances lead to the conclusion that extraterritoriality must be evaluated on an individual basis, the district court can decertify the class.

Second, Facebook argues that the district court abused its discretion by certifying the class because a class action is not superior to individual actions. According to Facebook, the possibility of a large, class-wide statutory damages award here defeats superiority.

We disagree. The question "whether the potential for enormous liability can justify a denial of class certification depends on [legislative] intent." *Bateman v. Am. Multi-Cinema, Inc.* (9th Cir. 2010). Where neither the statutory language nor legislative history indicates that the legislature intended to place a cap on statutory damages, denying class certification on that basis would "subvert [legislative] intent." Here, nothing in the text or legislative history of BIPA indicates that a large statutory damages award would be contrary to the intent of the General Assembly. Therefore, the district court did not abuse its discretion in determining that a class action is superior to individual actions in this case.

Notes

1. *Patel* shows how BIPA applies outside of the commonly litigated employment context. It links the concerns expressed by the Illinois legislature in 2008 to a long line of Fourth Amendment cases discussing concerns with technologically aided surveillance. And it gives us a peek into post-*Spokeo* standing doctrine.
2. Some plaintiff-side attorneys argue that federal standing is unimportant. Losing on federal standing does not end a case—it merely sends it to state court. And, given the choice between litigating in federal court in the Northern District of Illinois or in Madison County

state court, most defendants would happily choose federal court.[206] Some BIPA complaints are even drafted with a specific aim of *not* having federal standing.

Zellmer v. Meta, 104 F.4th 1117 (9th Cir. 2024)

R. NELSON, Circuit Judge:

Clayton Zellmer has never used Facebook. He sued Facebook—now Meta Platforms—for alleged violations of the Illinois Biometrics Information Privacy Act after his friends uploaded photographs of him to Facebook. He alleged that Facebook collected or captured his biometric identifiers when it created what Facebook calls a "face signature" from those uploaded photos. The district court granted summary judgment to Facebook on that claim. Zellmer also alleged that Facebook failed to publish a written policy establishing its retention schedule for collected biometric data. The district court dismissed that claim for lack of standing. We have jurisdiction under 28 U.S.C. § 1291, and we affirm.

I

Under the Illinois Biometrics Information Privacy Act (BIPA), a private entity can "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" only if it:

- Informs the subject or her representative in writing of the collection or storage of her biometric identifier or information;
- Informs the subject or her representative in writing of "the specific purpose and length of term" for their use; and
- Receives written authorization to do so from the subject or her representative.

740 Ill. Comp. Stat. 14/15(b) (Section 15(b)). A "biometric identifier" is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." As potentially relevant, biometric identifiers do not include photographs. For its part, "biometric information" is "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual" and "does not include information derived from items or procedures excluded under the definition of biometric identifiers."

Any company that possesses biometric identifiers or information must "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information (Section 15(a)). The required policy must clarify that any collected biometric identifier or information will be deleted "when the initial purpose" for the collection "has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." To ensure compliance, BIPA grants a "right of action" against an "offending party" to anyone aggrieved by a violation of its terms.

"In 2010, Facebook launched a feature called Tag Suggestions." *Patel v. Facebook, Inc.*, (9th Cir. 2019). If a user enables Tag Suggestions, Facebook "analyze[s] whether the user's Facebook friends are in photos uploaded by that user." If there is a match, then Facebook suggests that the user "tag" his friend. The Tag Suggestions feature proceeds in four steps.

---

[206] Madison County regularly ranks high on lists of plaintiff-friendly jurisdictions. *See, e.g.*, AMERICAN TORT REFORM FOUNDATION, EVERLASTING JUDICIAL HELLHOLES: A LONG, HOT 20 YEARS, https://www.judicialhellholes.org/hellhole/everlasting-judicial-hellholes/illinois/.

The first step is the Detection Stage. Facebook analyzes the photo to determine whether it includes any human faces. If Facebook detects a human face, it produces a cropped image of the face. Nothing more is done at this stage.

The next step is the Alignment Stage. Facebook takes any cropped image of a face and standardizes it by centering it, bringing it forward, and scaling it. Facebook is not always successful at standardizing a photo's detected faces. But if alignment is successful, then Facebook moves to the third step.

That step—which is the focus of this appeal—is the Representation Stage. Facebook tries to create what it calls a "face signature." A face signature is a string of numbers that represents a particular image of a face. Face signatures do not—and cannot—reveal information about a face's geometric information. And they neither reveal facial features nor the distances between them. They are simply numbers—an abstract, numerical representation of the aligned face crop created in previous stages. No one—not even Facebook—can reverse-engineer the numbers comprising a given face signature to derive information about a person. And even if the reverse-engineering of a face signature were technically possible, face signatures exist for only a tiny fraction of a second—they are neither saved nor stored after the final stage of the Tag Suggestions process.

The final step is the Classification Stage, which occurs immediately after a face signature is created. At this point, Facebook compares the face signature to what it calls face templates, which are only created for Facebook users. Facebook does not run the new face signature against every face template it has. Instead, it compares the face signature with the face templates of users who have both enabled face recognition and are connected to the user who uploaded the photo from which Facebook created the face signature. Regardless of whether the comparison yields a match, the face signature is immediately deleted.

After Zellmer's friends uploaded photos of him to Facebook, he sued Facebook (now Meta, which we use interchangeably) alleging violations of Sections 15(a) and 15(b) of BIPA by collecting, using, and storing biometric identifiers from photos without first obtaining written consent and establishing a public retention schedule.

After discovery, the district court granted summary judgment to Meta on Zellmer's Section 15(b) claim, finding that this statutory section did not protect the privacy interests of non-users. In the district court's view, "it would be patently unreasonable to construe BIPA to mean that Facebook was required to provide notice to, and obtain consent from, non-users who were for all practical purposes total strangers to Facebook, and with whom Facebook had no relationship whatsoever." The court considered this construction of Section 15(b) "untenable" because it deviated from the Illinois legislature's intent and would lead to absurd results, such as putting Meta in the "impossible position" of "obtain[ing] consent from every stranger whose face happened to be caught on camera." And that requirement would require Meta to abandon Tag Suggestions everywhere to avoid violating the law in Illinois. Such a result, the court explained, was impossible to square with the Supreme Court of Illinois's conclusion that BIPA "should not impose extraordinary burdens on businesses."

The district court denied Meta summary judgment on the Section 15(a) claim, finding that there is a factual dispute to be resolved at trial. A few months later, the district court addressed Zellmer's standing to bring a Section 15(a) claim. It held that Zellmer lacked Article III standing because he did not suffer a particularized injury and dismissed the Section 15(a) claim.

III

A

We begin by rejecting the grounds on which the district court granted summary judgment to Meta. The district court's decision turned on the practical impossibility of Meta's

complying with BIPA if it had to obtain consent from everyone whose photo was uploaded to Facebook before it could employ Tag Suggestions. Because the plain text applies to everyone whose biometric identifiers or information is held by Facebook, this conclusion was wrong.

"[W]hen the language of the statute is clear, it must be applied as written without resort to aids or tools of interpretation," "even though the consequences may be harsh, unjust, absurd or unwise," *Cothron v. White Castle Sys., Inc.*, (Ill. 2023).

Here, Section 15(b)'s language is clear: "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a *person's or a customer's*" biometric data without his consent. By delineating between persons and customers, BIPA shows that non-users are protected, regardless of any preexisting relationship with the party alleged to have violated BIPA. The only relevant question is whether Meta has collected or captured Zellmer's biometric data without his consent.

B

Having determined that BIPA protects users and non-users alike, we turn to whether there is a material dispute of fact as to whether Meta violated BIPA's plain terms. On the record before us, there is no dispute that Facebook made a face signature of Zellmer from photos that his friends uploaded. Our question, then, is whether a face signature is either a biometric identifier or biometric information for BIPA purposes. We conclude that it is neither.

1

Meta argues that BIPA applies only to biometric identifiers and information that can identify a person. Section 15(b) of BIPA protects not only "biometric information" that identifies an individual, but also "biometric identifiers" themselves. These "identifiers" are defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 Ill. Comp. Stat. 14/10. In other words, if either form of biometric data cannot identify an individual, it is not an identifier and thus not covered by BIPA. As evidence, Meta cites not only the dictionary definition of "identifiers," but also case law showing that biometric identifiers must be a feature that can identify a person. Zellmer responds that, while biometric information requires the ability to "identify an individual," biometric identifiers have no such explicit requirement. We join the other courts to have considered this issue and reject Zellmer's argument.

Zellmer would write the term "identifier" out of BIPA. Under his reading, every "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" is a biometric identifier and therefore within BIPA's reach. But this reading conflates necessary and sufficient conditions. The defined term imposes on the ordinary meaning of "biometric identifiers" a set of necessary conditions. Something that falls outside the defined statutory definition (such as a photograph) can be a biometric identifier under the term's plain meaning, but not be covered by BIPA's statutory definition. On the other hand, something can otherwise fall within BIPA's specific list of potential "biometric identifiers," but still not be covered if it cannot identify. For example, scans of face geometry fall within BIPA's list, but are not covered by BIPA if they cannot identify a person.

To understand why, we look to the Supreme Court's explanation that "[i]n settling on a fair reading of a statute, it is not unusual to consider the ordinary meaning of a defined term, particularly when there is dissonance between that ordinary meaning and the reach of the definition." *Bond v. United States* (2014). In *Bond*, the Court interpreted Congress's defined term "chemical weapon" against the backdrop of its ordinary meaning. In so doing, the Court concluded that the defendant did not engage in chemical warfare by using a chemical weapon when she "spread [common] chemicals on her car door, mailbox, and door knob" to cause her husband's mistress to "develop an uncomfortable rash." Even though the term "chemical weapon" included "toxic chemicals" such as those used by the defendant, "the global need to prevent chemical warfare does not require the Federal Government to reach into the kitchen

cupboard, or to treat a local assault with a chemical irritant as the deployment of a chemical weapon."

Applying that interpretive principle here, we conclude that the ordinary meaning of "identifier"—since it has an -er suffix—is "one that identifies." We are persuaded that the term's ordinary meaning informs its statutory meaning. As in *Bond*, where the statute's reach was limited by the term's ordinary meaning despite a statutory definition, applying the ordinary meaning of "identifier" would ensure that Meta is not forced to abandon key services that it offers its customers or risk perpetual liability. As Zellmer recognizes, these are the only two paths forward under his reading of the statute.

The list of "biometric identifiers" that the statute lists compels the same conclusion. Each of the listed items—retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry—are unique to a person. Each can thus be used to identify a person in the proper context. Generally, the words in a list should be given similar meanings. The unifying theme behind each term here is that each identifies a person.

Further, as Meta and amicus explain, BIPA's context supports a conclusion that "biometric identifiers" must identify. Take "biometric information." As Zellmer recognizes, unlike "biometric identifier," "biometric information" applies only to information "used to identify an individual." And Section 15(e) requires both identifiers and information to be afforded the protections given to "other confidential and sensitive information," defined as "personal information that can be used to *uniquely identify*" a person. Both terms thus turn on the ability to identify an individual. Reading the statute "as a whole," it makes sense to impose a similar requirement on "biometric identifier," particularly because the ability to identify did not need to be spelled out in that term—it was readily apparent from the use of "identifier."

Other courts have interpreted BIPA and reached the same conclusion. One such case, *Hazlitt v. Apple*, 500 F. Supp. 3d 738 (S.D. Ill. 2020), *judgment vacated on other grounds sub nom. In re Apple Inc.*, No. 20-8033, 2021 WL 2451296 (7th Cir. Jan. 22, 2021), is particularly persuasive since it was decided in Illinois on an issue of Illinois law. The *Hazlitt* plaintiffs alleged that Apple analyzed photographs saved to its Photo app to "specifically identify the Apple device user" and allowed users to tag "names for each of the faces detected in the People album" on the device. In its motion to dismiss, Apple argued that "these facial scans cannot qualify as biometric identifiers because Apple *does not* use the scans to actually identify a person." The *Hazlitt* court rejected Apple's interpretation as too narrow because "[t]he word 'identifier' modifies the word 'biometric' to signal that the types of data listed *could* be used to identify a person." *Hazlitt* thus recognized that, even if a company *does not* use face scans to identify a person, BIPA applies if it *could*. Given that understanding, the *Hazlitt* court denied the motion to dismiss because the complaint alleged "that the Photos app applies an algorithm to identify the device user," a fact that the court took "as true, at this stage." *Hazlitt* reflects the broad consensus that "biometric identifiers" under BIPA must be able to identify.

2

Meta's argument is different from Apple's in *Hazlitt*. Rather than arguing—like Apple—that Meta *does not* use the information it collected to identify anyone, Meta argues that the undisputed evidence shows that face signatures *cannot* identify non-users. Given our interpretation of "biometric identifiers" and the "biometric information" derived from them, if Meta is correct, then face signatures are not biometric identifiers or information under BIPA. The district court concluded, in a single sentence, that there was a dispute about whether face signatures can identify non-users. Having independently reviewed the record and the evidence cited by the parties, we conclude, contrary to the district court, that there is no material dispute of fact about whether face signatures can identify a person. We affirm the grant of summary judgment in Meta's favor on that basis.

To support its claim that face signatures are not biometric identifiers, Meta submitted a declaration from Gary McCoy, a Product Manager at Facebook. He explained that a face signature is merely "a string of numbers that represents a particular image of a face." Those numbers "do not reveal any geometric information about the detected face in the image, nor do they correspond to facial features like the eyes or nose, or distances between them." Instead, a face signature is "an abstract, numerical representation of a face crop that is computed by millions of pixel comparisons performed by the proprietary algorithm that Facebook has developed," which "cannot be reverse-engineered" and is neither "saved [n]or stored." Because the numbers that constitute a face signature cannot be reverse engineered, McCoy explained that "faces of non-users ... that appear in photos are anonymous to Facebook" and that "it is not possible to identify" non-users from their face signatures. The creation of face signatures "do[es] not create or store any other data from the detected faces of non-users ... that could be used to recognize or identify them through the use of face recognition."

To dispute the McCoy declaration, Zellmer offers evidence that the face signature can predict a person's age and gender and that Meta turns on what is called the "recognizable indicator," which is "associated with a given face," for face signatures. Finally, he notes that face signatures "include the geometric x and y coordinates within the photo where a person's face appears, thus calculating the dimensions of the person's face."

Neither piece of evidence can carry the weight Zellmer affords it. That a face signature can predict a person's gender limits the pool of potential matches to approximately 50% of the population; this fails to identify anyone. Nor is a person's age—standing alone or together with his or her gender—able to identify a person. Nor is the gender-identification always accurate: Zellmer himself erroneously matched to a woman from the face signatures that Meta created. As for the recognizable indicator being turned on, this means only that the image can advance to the standardization phase—Meta's process for determining whether it can create a face signature. Put differently, the recognizable indicator allows Meta only to identify that a particular image contains a face. But this does not mean that Meta can, from that face, identify a person. Nor do the coordinates within the photos that can map out the size of a person's face show that Meta can, from those coordinates, identify an unknown person.

These are the three key facts which Zellmer relied on below. And he points to no new evidence in the record on appeal. None of these facts rebuts Meta's showing that a face signature, which is all that was ever created for Zellmer, cannot identify him.

IV

We also affirm the district court's dismissal of the Section 15(a) claim for lack of standing. Zellmer alleges that Meta lacks written, publicly available policies identifying its retention schedules for permanently destroying any biometric identifiers or information of non-users like him in its possession.

Article III's "case or controversy" requirement "limits federal courts' subject matter jurisdiction by requiring, inter alia, that plaintiffs have standing." A plaintiff must demonstrate standing by establishing (1) an injury in fact (2) fairly traceable to the defendant's challenged conduct (3) that is likely to be redressed by a favorable decision. A plaintiff shows injury in fact if he has "suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.' "

These well-trodden principles compel our conclusion that Zellmer lacks standing to bring his Section 15(a) claim. Zellmer alleges a single sentence about Section 15(a): "Facebook does not publicly provide a retention schedule or guidelines for permanently destroying the biometric identifiers and/or biometric information of Plaintiff and the Class members." But as the Seventh Circuit has concluded, this is a duty owed not to any particular person, but to the "public generally." *Bryant v. Compass Grp. USA,* (7th Cir. 2020).

Zellmer never explained how he or any of the proposed class members are harmed by violations of this general duty in a "concrete and particularized" way. Nor could he have, given our conclusion that—on the record before us—face signatures are not biometric identifiers or information. As a result, Meta's creation of face signatures does not lead to the "very substantive harm targeted by BIPA." And, as Zellmer concedes, if there is no Section 15(b) violation, he lacks standing to bring a Section 15(a) claim. Because face signatures are neither biometric identifiers nor information, Zellmer is no more harmed by Meta's failure to have a retention schedule or guidelines related to the destruction of biometric identifiers or information than anyone else in Illinois.

Our decision in *Patel* is not to the contrary. There, we held that BIPA established "concrete interests" in privacy, not merely procedural rights. We then considered whether the violations Patel alleged harmed those concrete interests. We concluded that they did. In so concluding, we explained that plaintiffs alleged that Facebook created a "face template" of them from uploaded photos, the "very substantive harm targeted by BIPA." Zellmer has not shown that his BIPA data was ever in Meta's possession or that he has been harmed in a particularized way different from the public generally. Thus, *Patel* does not resolve the allegations here.

Notes

1. In the eyes of the court, a face signature is different than a face template. Face templates are biometric identifiers, according to *Patel,* and are created only for Facebook users. Face signatures are created in response to all uploaded photographs, including those depicting nonusers such as the plaintiff here. Face signatures are highly temporary and, according to the court, do not contain identifiable information. Does that strike you as correct? What should we make of the fact that a face signature can be compared to face templates, allowing the system to determine if the face signature matches particular enrolled facial images? A face signature of an enrolled user – one who has a face template – could be used to identify them. Is such a face signature a biometric identifier under BIPA? Could two facial signatures themselves be compared?
   There are two issues here. First, does one fully credit the declaration from Gary McCoy stating that identification is not possible from the facial signature? A more thorough development of the record here would have been appreciated. Second, if one does credit the declaration, does it matter? This gets at a hard and recurring issue in biometric privacy law: the problem of negative matches. Imagine a person has been banned from a store and, in the process of being banned, signed a document giving the store permission to use their biometrics to detect their presence. Perhaps this was in exchange for not prosecuting them for shoplifting. If the store uses facial recognition to scan for this person, it will inevitably collect – and perhaps immediately discard – the facial signatures of countless nonconsenting people. Is that okay?
2. What do you make of the 9th Circuit's treatment of the *Hazlitt* decision? In *Hazlitt*, information was held to be a biometric identifier because it could be used to uniquely identify a person even if it was not. The 9th Circuit interprets that to mean that the ability to uniquely identifier a person is an inherent part of the definition of biometric identifier.
3. A line of cases has considered whether video filters that superimpose various things on a person's face – bunny ears, cat whiskers, and the like – are collecting biometrics. These cases sometimes survive motions to dismiss. For example, in *Hartman v. Meta Platforms, Inc.*, 2024 WL 4213302, at *11 (S.D. Ill. Sept. 17, 2024), the court stated:

   > Affording the complaint the generous interpretation to which it is entitled, the Court finds that it sufficiently alleges that Meta scanned users' face geometries and that these scans are capable of identifying the people from whom they were taken. Plaintiffs allege that the Messenger Applications relied on AR technology to create "scans of face geometry to identify individuals' location[s], expressions, and movements" in real time. The resulting facial geometry scans "model[ed]

> users [sic] faces" based on an "estimation of the location of parts of [their] faces." These allegations permit an inference of personalization that supports the uniqueness of each scan based on the user from whom it was taken.

Both whether this scan was sufficient to count as a biometric and whether Meta could fairly be said to have collected the biometric – was the resultant information only on the user's device, or was it shared with Meta? – were both issues to resolve in discovery.

4. There is a growingly convoluted doctrine of BIPA standing. Subsequent to the *Hazlitt* decision the 7th Circuit held that some violations of 15(a) do grant federal standing, specifically those that allege that data retention schedules are not *complied with* in addition to not being disclosed to the public, meaning that an individual's data is not deleted. *Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146 (7th Cir. 2020). But given that deletion was immediate here, that distinction is not relevant in *Zellmer*.

BIPA cases also raise the question of how to "count" violations. Take the example of 200 employees clocking into work on a biometric timeclock. Is that 200 violations total, one for each employee? Or 200 violations per day the timeclock is used? The latter interpretation leads to a frightening result. 200 employees multiplied by approximately 250 workdays in a year is 50,000 violations per year. At $1,000 per violation, the company would be liable for $50 million.

In *Cothron v. White Castle System, Inc.* (Ill. 2023), the Illinois Supreme Court held that each individual scan was its own violation. This both refreshed the statute of limitations for the person scanned (the key issue in the case), as well as opened the door to the possibility of multiple recoveries for each person. BIPA was subsequently amended to restrict each plaintiff to a single recovery, but the policy arguments below are still relevant, as is the examination of how class action damages should be considered.

Cothron v. White Castle System, Inc., 216 N.E.3d 918 (Ill. 2023)

JUSTICE ROCHFORD delivered the judgment of the court, with opinion.

[After reviewing a textual argument that the court concluded allowed for each collection to count as a separate violation]

We are not persuaded by White Castle's nontextual arguments in support of its single-accrual interpretation.

[C]ontrary to White Castle's position, *Rosenbach* does not stand for the proposition that the "injury" for a section 15 claim is predicated on, or otherwise limited to, an initial loss of control or privacy. Instead, *Rosenbach* clearly recognizes the statutory violation itself is the "injury" for purposes of a claim under the Act, which is entirely consistent with our decision here. Our subsequent decisions in *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc.* (Ill. 2021) and *McDonald v. Symphony Bronzeville Park, LLC* (Ill. 2022) adhered to *Rosenbach*'s construction of the Act and similarly recognized that a claim under the Act is a private cause of action based exclusively on a statutory violation.

White Castle and *amici* supporting White Castle's position caution this court against construing section 15(b) and section 15(d) to mean that a claim accrues for each scan or transmission of biometric information made in violation of those provisions. They assert that, because section 20 of the Act sets forth liquidated damages that a party may recover for "each violation," allowing multiple or repeated accruals of claims by one individual could potentially result in punitive and "astronomical" damage awards that would constitute "annihilative liability" not contemplated by the legislature and possibly be unconstitutional. For example, White Castle estimates that if plaintiff is successful and allowed to bring her claims on behalf of as many as 9,500 current and former White Castle employees, class-wide damages in her action may exceed $17 billion. We have found, however, that the statutory language clearly

supports plaintiff's position. As the district court observed, this court has repeatedly held that, where statutory language is clear, it must be given effect, "'even though the consequences may be harsh, unjust, absurd or unwise.'"

This court has repeatedly recognized the potential for significant damages awards under the Act. This court explained that the legislature intended to subject private entities who fail to follow the statute's requirements to substantial potential liability. The purpose in doing so was to give private entities "the strongest possible incentive to conform to the law and prevent problems before they occur." As the Seventh Circuit noted, private entities would have "little incentive to course correct and comply if subsequent violations carry no legal consequences."

All of that said, we generally agree with our appellate court's recognition that "[a] trial court presiding over a class action—a creature of equity—would certainly possess the discretion to fashion a damage award that (1) fairly compensated claiming class members and (2) included an amount designed to deter future violations, without destroying defendant's business." It also appears that the General Assembly chose to make damages discretionary rather than mandatory under the Act. See 740 ILCS 14/20 (detailing the amounts and types of damages that a "prevailing party *may* recover" (emphasis added)). While we explained in *Rosenbach* that "subjecting private entities who fail to follow the statute's requirements to substantial potential liability, including liquidated damages, injunctions, attorney fees, and litigation expenses 'for each violation' of the law" is one of the principal means that the Illinois legislature adopted to achieve the Act's objectives of protecting biometric information, there is no language in the Act suggesting legislative intent to authorize a damages award that would result in the financial destruction of a business.

In sum, we conclude that the plain language of section 15(b) and 15(d) shows that a claim accrues under the Act with every scan or transmission of biometric identifiers or biometric information without prior informed consent.

JUSTICE OVERSTREET, dissenting:

Turning to the language of the statute, section 15(b) requires certain disclosures to be made, and a written release obtained, before that entity may "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information." The statute thus broadly applies to any way that a private entity obtains a person's or customer's biometric information without consent. It is axiomatic, however, that a private entity may obtain any one type of a person's biometric information only once, at least until that biometric identifier or information is destroyed. With subsequent authentication scans, the private entity is not obtaining anything it does not already have.

The analysis is the same for section 15(d) claims. Under section 15(d), a private entity in possession of a person's biometric identifier or information must obtain that person's consent before it may "disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information." With respect to any one party to whom the biometric information is disclosed, the person loses control of her biometric identifier or information only once. There is no further loss of control, privacy, or secrecy with subsequent provision of the identical biometric information to the same party.

The majority acknowledges that, in construing the Act as it has, the consequences may be harsh, unjust, absurd, or otherwise unwise. In doing so, the majority ignores that the construction of a statute that leads to an absurd result must be avoided. Instead, a court construing the language of a statute should "'assume that the legislature did not intend to produce an absurd or unjust result' and [should] avoid a construction leading to an absurd result, if possible."

In considering the consequences of construing the Act one way or another and giving each word of the statute a reasonable meaning, two significant consequences militate against

the majority's construction. First, under the majority's rule, plaintiffs would be incentivized to delay bringing their claims as long as possible. If every scan is a separate, actionable violation, qualifying for an award of liquidated damages, then it is in a plaintiff's interest to delay bringing suit as long as possible to keep racking up damages. Because there is no additional loss of privacy, secrecy, or control once a private entity has obtained a person's biometric information, the plaintiff loses nothing by waiting to bring suit until as many scans as possible are accumulated. This point, all by itself, should convince the majority that its interpretation is wrong. If, indeed, a party *was* losing control over his or her biometric information with every scan, this incentive would simply not exist.

Next, the majority's construction of the Act could easily lead to annihilative liability for businesses. As the Seventh Circuit explained:

> "White Castle reminds us that the Act provides for statutory damages of $1,000 or $5,000 for 'each violation' of the statute. Because White Castle's employees scan their fingerprints frequently, perhaps even multiple times per shift, Cothron's interpretation could yield staggering damages awards in this case and others like it. If a new claim accrues with each scan, as Cothron argues, violators face potentially crippling financial liability."

The majority acknowledges White Castle's estimate that, if plaintiff is successful in her claims on behalf of as many as 9,500 current and former White Castle employees, damages in this action may exceed *$17 billion*. Nevertheless, the majority brushes this concern aside by stating that "policy-based concerns about potentially excessive damage awards under the Act are best addressed by the legislature."

Notes

1. In 2024, the Illinois legislature amended BIPA to state that an "aggrieved person is entitled to, at most, one recovery under this Section." This is the first amendment to BIPA since its passage.
2. The case effectively holds that scanning a biometric to compare it to a previously collected image is a collection of a biometric. Consider again the example of the shoplifter from the note following *Zellmer*. Imagine that a store "trespasses" a shoplifter; tells them that they are not welcome there and that the police will be called if they enter again. The shoplifter signs a document confirming their understanding of this and granting permission for biometric scanning. If the store then scans for them, it is collecting their biometric again and again; that is the direct holding of *White Castle*. But is it also collecting the biometric of everyone else in the store, even if it immediately deletes the data after not finding a match? In each case it is not permanently storing novel data.
3. The flood of litigation from BIPA comes from the combination of its broad scope, statutory damages, and private right of action. Consider by contrast the Texas statute, Capture or Use of Biometric Identifier ("CUBI"). As with BIPA, CUBI defines "biometric identifier" broadly as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." Texas Business and Commerce Code § 503.001(a). It then states:

> (b) A person may not capture a biometric identifier of an individual for a commercial purpose unless the person:
>
> (1) informs the individual before capturing the biometric identifier; and
>
> (2) receives the individual's consent to capture the biometric identifier.
>
> (c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose:
>
> (1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:

> (A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death;
>
> (B) the disclosure completes a financial transaction that the individual requested or authorized;
>
> (C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or
>
> (D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant;
>
> (2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses; and
>
> (3) shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1).

These provisions are similar to BIPA in many ways. Consent must be obtained before biometric data is collected and, once collected, the biometric data cannot be further shared or disclosed. Notably, however, consent need not be in writing, the notice to the individual does not have to be as detailed, and there is no private right of action. Only the Texas Attorney General can bring an action under the statute. Thus far, only a handful of such suits have been filed. The first of these were targeted at Google and Meta over facial recognition use. Meta settled its lawsuit in 2024 for $1.4 billion. Google subsequently settled this and other claims for 1.3 billion.

F. Comprehensive State Privacy Laws

Thus far, we have seen that the protections offered to consumer data tend to be highly limited and sectoral. There is no general federal consumer privacy statute nor does the Federal Trade Commission, despite its large role in the privacy space, provide an all-encompassing substitute for such a thing. States, however, have taken the lead in the consumer privacy space. Most notable in this regard is the California Consumer Privacy Act ("CCPA").

1) California Consumer Privacy Act

The CCPA was originally proposed as a ballot initiative in 2017 by Californians for Consumer Privacy, an activist group chaired by real estate developer Alastair Mactaggart. After negotiating with that group, however, the California legislature passed it into law itself in 2018 with an effective date of 2020. Enacting the CCPA via the legislature had the benefit of allowing for future legislative amendments; ballot initiatives are hard to amend absent future ballot initiatives. Therefore, the drafting and passage of the CCPA was rather rushed, especially when one considers that it was likely the most important piece of American privacy legislation passed in that decade. Unhappy with the legislature's later tinkering with the CCPA, Californians for Consumer Privacy sponsored a new ballot initiative, the California Privacy Rights Act (CPRA), in the 2020 election cycle. This passed with 56% of the vote. For simplicity's sake, the combined CCPA-CPRA is referred to as the CCPA.

Scope. The CCPA applies to for-profit businesses that do business in California and meet any of the following requirements:

1. Have a gross annual revenue of over $25 million;

2. Buy, sell, or share the personal information of 100,000 or more California residents, households, or devices; or
3. Derive 50% or more of their annual revenue from selling California residents' personal information.

CAL. CIV. CODE §§ 1798.140(d)(1)(A)–(C). This, therefore, exempts both nonprofits and most small businesses, though small data-driven businesses qualify if they have data on 100,000 or more Californians and engage in any of the "buy, sell, or share" activities. Sharing may seem uncommon, but it is defined broadly in the CCPA as "sharing, renting, . . . disclosing . . . or otherwise communicating . . . a consumer's personal information . . . to a third party for cross-context behavior advertising, whether or not for monetary or other valuable consideration." § 1798.140(ah)(1). So, even data sharing for traditional targeted advertising qualifies.

The goal of the CCPA's scope limitation is to avoid putting too great a strain on companies that cannot afford to follow the CCPA and likely do not pose a major privacy burden on California consumers anyway. These limitations mark a sharp contrast to Illinois' Biometric Information Privacy Act, which applies to all private actors. The CCPA also does not apply to HIPAA covered data, data subject to the Gramm Leach Bliley Act (GLBA), or data held and shared by consumer reporting agencies as regulated by the Fair Credit Reporting Act. Note that the these exceptions are specifically for the covered "data" not the covered "entity." So a GLBA entity in possession of non-GLBA covered data still needs to comply for the purposes of that non-GLBA data.

Personal Data. The protections of the CCPA apply to "personal information," which is defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." § 1798.140(v)(1). The statute explicitly includes biometric information; identifiers such as name, alias, postal address, and government ID number; geolocation information; internet or network activity information; inferences about consumer preferences, attitudes, and beliefs; and characteristics protected under California or federal law. §§ 1798.140(v)(1)(A)–(L). Therefore, the definition of personal information is incredibly broad, and even inferences about consumer behavior are included.

Exempted from the definition of personal data are a variety of categories of information:

1. Publicly available information, which means information lawfully available from federal, state, or local government records; or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. This definition does not include biometric information collected by a business about a consumer without the consumer's knowledge.
2. Lawfully obtained, truthful information that is a matter of public concern.
3. Consumer information that is deidentified or aggregated.

CIV. §§ 1798.140(v)(2)–(3). So publicly available information includes publicly recorded property records, public criminal history information, and any other individual information made available by the government. It also includes public social media postings and news reports. It does not include a biometric scan of a consumer's face, even if the consumer is in a public setting. However, it does include the consumer's general appearance in public. Further, deidentified or aggregated information does not receive protection, though that raises the further issue of what counts as sufficiently deidentified.

Consumer Rights. Substantively, the CCPA grants California consumers a series of key rights:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale or sharing of their personal information;
- The right to nondiscrimination for exercising their CCPA rights;
- The right to correct inaccurate personal information that a business has about them; and
- The right to limit the use and disclosure of sensitive personal information collected about them.

These rights are complex. Consider the right to know. How much must consumers be told? How easily must this information be accessible? How must consumers be updated when a business's information practices change? Therefore, let us consider each right one by one.

Right to Know. This right comes in two flavors. First, a business must make the following information publicly accessible: the categories of personal information it collects, the sources of that information, the general purpose in collecting the information, and the categories of third parties with which it is shared. § 1798.110(c). Second, consumers must be able to request that the business reveal to them the specific pieces of information that the business has collected from the consumer. § 1798.110(a). This, for instance, would include having Meta disclose every Facebook post, personal message, like, and comment a person has made that still exists on Meta's servers.[207]

The right to know and several other rights require a person to submit a "verified" request. In short, the business needs to know that the person making the request is the same as the person the request is about. § 1798.110(c). There are a host of rules about verifying requests. For example, a company cannot require you to create an account to file a request under the CCPA, and it generally must provide multiple methods of verifying identities. § 1798.130(a)(1)(A).

Right to Delete. This right appears simple: a person may request that a business delete the information the business has collected from them. § 1798.105(a). Upon receiving such a request, the business must delete the information unless it falls into one of several exceptions. CIV. 1798.105(c)–(d). If the business invokes an exception to avoid deleting data, it must limit its future use of that data to be consistent with the exception used. The challenge is the broad scope of the right-to-delete exceptions. A business may refuse to delete information that is not covered by the CCPA, such as publicly available information. It may also retain information that it needs to complete a pending transaction or continue to provide a product or service to the consumer; for business security purposes (think cybersecurity and investigation); to comply with legal obligations; or to make any other use that is compatible with reasonable consumer expectations or the context in which the information was provided. § 1798.105(d).

Consider the broad scope of the legal-obligations exception. For tax purposes, a business needs to know what it sold and, to some extent, to whom. Without customers' personal information to explain the source of revenue, a business may be accused of money laundering. State laws also require businesses to keep records of the sales of certain products for recall notices, and warranty programs require similar records.

The other exceptions are similarly broad. Deidentified data is outside the scope of the CCPA and can be retained. Reasonable consumer expectations are nebulous and arguably justify a great deal of data collection and retention. Cybersecurity purposes can be used to justify the short-term retention of much website data.

---

[207] As of this writing, the Facebook help page explaining how to make that request is located here: https://www.facebook.com/help/212802592074644.

Right to Opt Out. Consumers can demand that a business stop selling or sharing their personal information. § 1798.120(a). This includes use in cross-context behavioral advertising (see *Sephora* below). Recall that sharing is broadly defined. Upon receiving such a request, businesses are supposed to stop selling or sharing information unless the consumer grants fresh consent, § 1798.120(d), and the business cannot ask for fresh consent for at least 12 months, § 1798.135(c)(4). Businesses can deny these requests when they need to continue to share information to comply with legal obligations.

The CCPA further regulates the ways in which the right to opt out must be presented to consumers. For example, a web-based business shall post a notice on a "Do Not Sell My Personal Information" page. § 1798.185(a)(19)(A)(vi)(III). A brick-and-mortar establishment must provide an in-person equivalent.

Right to Nondiscrimination. Businesses cannot deny goods or services, charge a different price, or provide a different level or quality of goods or services just because a person has exercised their rights under the CCPA. § 1798.125(a)(1). Still, exercising rights may require a person to leave certain business programs, such as a customer loyalty program, or make it impossible to complete other transactions. § 1798.125(a)(2). Further, businesses can offer incentives for being allowed to collect, keep, or sell personal information provided the value of those incentives is reasonably related to the value of the personal information. § 1798.125(a)(3).

Current CCPA regulations[208] offer four examples of these principles:

> *Example 1*: A music streaming business offers a free service as well as a premium service that costs $5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale or sharing of their personal information, then the practice is discriminatory, unless the $5-per-month payment is reasonably related to the value of the consumer's data to the business.
>
> *Example 2*: A clothing business offers a loyalty program whereby customers receive a $5-off coupon by email after spending $100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code § 1798.105(d)(1).
>
> *Example 3*: A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale/sharing of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.
>
> *Example 4*: An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the

[208] CCPA REGS. TIT. 7 § 7080(d), https://cppa.ca.gov/regulations/pdf/20230329_final_regs_text.pdf.

> value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

Right to Correct. Consumers have the right to demand that companies correct inaccurate information in their records. § 1798.106(a). Businesses can deny the request if they determine that the information is more likely than not correct. § 1798.185(a)(8). Currently, this right is the subject of rulemaking, and not much is known about the exact contours of this process.

Right to Limit the Use and Disclosure of Sensitive Personal Information. Consumers may request that companies limit their use of sensitive personal information (for example, social security number, financial account information, precise geolocation data, or genetic data) to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services with some narrowly tailored exceptions. § 1798.121(a). A business receiving such a request must comply and notify their service providers so they may comply as well. § 1798.121(b).

The exceptions here are more limited than those of the right to delete. They include continuing uses that are required by law; uses to protect either the security of the business or of natural persons; uses to provide customer service functions such as servicing accounts; and uses that are not for the purpose of inferring characteristics about people. §§ 1798.121(a), (d). As an example of the last of these, the regulations offer:

> [A] business that includes a search box on their website by which consumers can search for articles related to their health condition may use the information provided by the consumer for the purpose of providing the search feature without inferring characteristics about the consumer. CCPA REGS. TIT. 11 § 7027(m)(8).

Enforcement. The CCPA is enforced both by the California Attorney General's office and the newly created California Privacy Protection Agency (CPPA). § 1798.155(a). If a violation occurs, the CPPA may fine a company $2,500 per violation or $7,500 per intentional violation (subject to later judicial review). The California Attorney General can bring a civil action. There is no private right of action except for data breach (described below). Previously there was a 30-day cure period, allowing companies to retrospectively come into compliance with the CCPA after being notified of an issue. But that period was removed by the CPRA in 2023.

Data Breach. Businesses under the CCPA have an obligation to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." § 1798.150(a)(1). If unencrypted and nonredacted information is breached due to a business's failure to adopt such security measures, consumers can sue either individually or as part of a class action. The data breach provision allows for statutory damages of between $100 and $750 per person or actual damages. § 1798.150(a)(1)(A).

To qualify as a data breach, particular categories of personal information need to have been exposed. § 1798.81.5(d)(1)(A). Specifically, it counts as a breach under the CCPA when an individual's first name or first initial and last name are exposed in combination with: their social security number; other government ID number; account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; health insurance information; or biometric or genetic information. § 1798.81.5(d)(1)(A).

California v. Sephora USA, Inc. (Cal. Super. Ct. 2022)

Complaint for Injunction, Civil Penalties, and Other Equitable Relief

Consumers are constantly tracked when they go online. Sephora, like many online retailers, installs third-party companies' tracking software on its website and in its app so that these third parties can monitor consumers as they shop. The third parties track all types of data; in Sephora's case, third parties can track whether a consumer is using a MacBook or a Dell, the brand of eyeliner that a consumer puts in their "shopping cart," and even the precise location of the consumer. Some of these third-party companies create entire profiles of users who visit Sephora's website, which the third parties then use for Sephora's benefit. For example, the third party might provide detailed analytics information about Sephora's customers and provide that to Sephora, or offer Sephora the opportunity to purchase online ads targeting specific consumers, such as those who left eyeliner in their shopping cart after leaving Sephora's website. This data about consumers is frequently kept by companies and used for the benefit of other businesses, without the knowledge or consent of the consumer.

The ramifications of this third-party surveillance can go beyond ordinary consumer profiling. Sephora's website allows visitors to browse and purchase products such as prenatal and menopause support vitamins—data points which can be used by third-party companies to infer conclusions about women's health conditions, like pregnancy. Moreover, when a company like Sephora utilizes third-party tracking technology without alerting consumers and giving them the opportunity to control their data, they deprive consumers of the ability to limit the proliferation of their data on the web.

California's landmark privacy law, the CCPA, sought to prevent this. Thanks to the CCPA, Californians now have rights over their personal information, including the right to access and delete personal information and the right to opt-out of the sale of personal information. The right to opt-out is the hallmark of the CCPA. This right requires that companies follow certain straightforward rules: if companies make consumer personal information available to third parties and receive a benefit from the arrangement—such as in the form of ads targeting specific consumers—they are deemed to be "selling" consumer personal information under the law. This in turn triggers certain basic obligations, including that the business tell consumers that it is selling their personal information and allow consumers to opt-out of those sales, such as by clicking an easy-to-find "Do Not Sell My Personal Information" link.

Sephora did not do this. Sephora did not tell consumers that it sold their personal information; instead, Sephora did the opposite, telling California consumers on its website that "we do not sell personal information." Sephora also did not provide consumers with an easy-to-find "Do Not Sell My Personal Information" link, either on its webpage or in its app.

To help consumers who want to easily opt-out, the CCPA requires that a business take steps to ensure that any user who has "user-enabled global privacy controls" is treated the same as users who have clicked the "Do Not Sell My Personal Information" link. This requirement was intended to spur innovation and encourage the development of technologies that would allow consumers to universally opt-out of all online sales in one fell swoop, giving consumers the agency and ability to stop their data from being sold over and over again. With a universal opt-out, consumers can broadcast a "do not sell" signal across every website they visit, without having to click each time on an opt-out link. But again, Sephora failed to honor this requirement. Sephora's website was not configured to detect or process any global privacy control signals, such as the "Global Privacy Control" (GPC). As a result, Sephora wholly disregarded consumers who communicated to the company, via a global opt-out signal, that Sephora should not sell their personal information.

The Attorney General notified Sephora of these violations. Under the CCPA, Sephora had 30 days to cure. After Sephora failed to cure any of the alleged violations, the Attorney General initiated an in-depth investigation leading to this enforcement action.

Sephora is a beauty retailer that sells products through its website, mobile application, and brick-and-mortar stores throughout California. When Sephora sells products online, it collects personal information about consumers. This information includes the products that consumers view and purchase, consumers' geolocation data, cookies and other user identifiers, and technical information about consumers' operating systems and browser types.

Sephora also makes consumers' personal information available to third-party companies for the purpose of obtaining advertising and analytics. In its privacy policy dated June 18, 2021, Sephora admitted that it shared consumers' geolocation data and "[i]nternet or other electronic network activity information" with third parties, including "advertising networks, business partners, data analytics providers," and others. Sephora made this data available to these companies by installing (or allowing the installation of) third-party trackers in the form of cookies, pixels, software development kits, and other technologies, which automatically send data about consumers' online behavior to the third-party companies.

Sephora's decision to provide third parties including "advertising networks, business partners, [and] data analytics providers" with access to its customers' data in exchange for services from those entities was a sale of personal information as defined by the CCPA. Section 1798.140, subdivision (t), broadly defines sales as the exchange of personal information for anything of value. Sephora's relationships with these third parties met that definition, because Sephora gave companies access to consumer personal information in exchange for free or discounted analytics and advertising benefits. For example, Sephora installed one widely-used analytics and advertising software package that let the analytics provider gather and keep personal information about an online shopper's activities. The analytics provider then gave Sephora data about what shoppers did on its website or in its app, like how many people looked at a particular product. The analytics provider also would determine who the shopper was, using extensive data gathered from other sources, and then present Sephora with the valuable option to serve targeted advertisements to the same shopper on the analytics provider's advertising network. Both the trade of personal information for analytics and the trade of personal information for an advertising option constituted sales under the CCPA.

Sephora installed and used other widely available advertising and analytics services from companies with which Sephora had the same fundamental deal: Sephora allowed the third-party companies access to its customers' online activities in exchange for advertising or analytic services. Sephora knew that these third parties would collect personal information when Sephora installed or allowed the installation of the relevant code on its website or in its app. Sephora also knew that it would receive discounted or higher-quality analytics and other services derived from the data about consumers' online activities, including the option to target advertisements to customers that had merely browsed for products online. Sephora also did not have valid service-provider contracts in place with each third party, which is one exception to "sale" under the CCPA. All of these transactions were sales under the law.

In June 2021, the Attorney General commenced an enforcement sweep of large retailers to determine whether they continued to sell personal information when a consumer signaled an opt-out via the GPC. In part, the testing and investigation used commercially available browser extensions to monitor network traffic involving third-party advertising and analytics providers, and analyzed how that traffic changed when the GPC sent its "do not sell" signal. In investigating Sephora's website, the Attorney General found that activating the GPC had no effect and that data continued to flow to third-party companies, including advertising and analytics providers. Subsequent testing confirmed that Sephora's website took no action to block the transmission of personal information even when a California consumer signaled their opt-out using the GPC. In short, Sephora completely ignored the GPC.

The Attorney General also found other sale-related violations. Because Sephora sold personal information, the CCPA required Sephora to undertake several compliance obligations.

- First, Sephora was required to notify consumers of the "the categories of personal information [Sephora] has sold or shared about consumers in the preceding 12 months." Sephora failed to make these disclosures or give consumers these material facts in its separate portion of the privacy policy titled "Information for California Residents." In that California-specific notice, Sephora merely noted that it "share[d]" personal information and provided consumers with a link to see what information was shared. Upon clicking that link, Sephora expressly told consumers "that we do not sell personal information."
- Second, Sephora was required to post a "Do Not Sell My Personal Information" link on its website and in its mobile application as well as provide another means of opting out. Sephora failed to offer any means of opting out.
- Third, for consumers who exercised their right to opt-out of the sale of their personal 10 information, Sephora was required to refrain from selling that data. This includes consumers who exercise their right to opt-out via a user-enabled global privacy control. Instead, Sephora sold the personal information of consumers who exercised their right to opt-out via the GPC.

On June 25, 2021, the Attorney General notified Sephora that it may be in violation of the CCPA and had 30 days to cure before it faced legal liability. Sephora did not cure any of the alleged violations.

FIRST CAUSE OF ACTION

(Failure to Notice Sale of Consumer Personal Information, Provide "Do Not Sell My Personal Information" Link, Provide Two Or More Methods to Opt-Out of Sale, and Process Requests to Opt-Out Via User-Enabled Global Privacy Controls)

Sephora's website and mobile app failed to inform consumers that it sells their personal information and that they have the right to opt-out of this sale, failed to provide a clear and conspicuous "Do Not Sell My Personal Information" link that would enable a consumer to opt-out of the sale of their personal information, and failed to provide two or more designated methods for submitting requests to opt-out.

Accordingly, each time a Californian visited Sephora's website beginning on July 25, 2021, Sephora violated:

(a) Civil Code section 1798.130, subdivision (a)(5);

(b) Civil Code section 1798.135, subdivision (a)(1);

(c) California Code of Regulations, title 11, sections 7010, 7011, 7013, and 7026.

In addition, for consumers who enabled the GPC, Sephora violated Civil Code section 1798.120, subdivision (a), section 1798.135, subdivision (a)(4), and California Code of Regulations, title 11, section 7026, subdivision (c)(1), by failing to treat the GPC as a consumer's opt-out of the sale of their personal information and continuing to sell personal information to third parties despite receiving a GPC signal.

Upon the Attorney General providing notice of these violations of the CCPA, and implementing regulations, Sephora failed to cure them within 30 days. Each time Sephora failed to stop the sale of data to a third party, Sephora violated the law.

SECOND CAUSE OF ACTION

(Failure to Process Requests to Opt-Out Via User-Enabled Global Privacy Controls)

Sephora has engaged in unlawful, unfair, or fraudulent acts or practices, which constitute unfair competition within the meaning of Section 17200 of the Business and Professions Code. Defendants' acts or practices include, but are not limited to, making false or misleading statements of facts concerning Defendants' sale of consumers' personal information and unfairly depriving consumers of the ability to opt-out of this sale.

Final Judgement and Permanent Injunction, California v. Sephora USA, Inc. (Cal. Super. Ct. Aug. 24, 2022)

DEFENDANT shall comply with [the CCPA].

To the extent DEFENDANT SELLS the PERSONAL INFORMATION of CONSUMERS, including through SALES USING ONLINE TRACKING TECHNOLOGY, DEFENDANT shall provide notice to CONSUMERS as required by Civil Code section 1798.135, subdivision (a) that clearly states that it SELLS their PERSONAL INFORMATION, and that CONSUMERS have the right to opt-out of all SALES.

DEFENDANT shall process CONSUMER requests to opt out signaled via the Global Privacy Control or the "GPC."

Within 180 days of the EFFECTIVE DATE, and for a period of 2 years thereafter, DEFENDANT shall implement and maintain a program to assess and monitor whether it is effectively processing the requests of CONSUMERS to opt-out of the SALE of their PERSONAL INFORMATION, including requests submitted via user-enabled global privacy controls like the Global Privacy Control ("GPC"). DEFENDANT shall share its assessment with the People in an annual report, that includes the following:

a. A detailed overview of the testing DEFENDANT has done to assess and monitor its processing of CONSUMER requests to opt-out of the SALE of their PERSONAL INFORMATION submitted via user-enabled global privacy controls like the Global Privacy Control ("GPC").
b. An analysis of any errors or technical problems encountered by DEFENDANT in processing CONSUMER requests to opt-out of the SALE of their PERSONAL INFORMATION via user-enabled global privacy controls like the Global Privacy Control ("GPC"), if any, and steps taken by DEFENDANT to fix or remediate those errors or problems.

Within 180 days of the EFFECTIVE DATE, and for a period of 2 years thereafter, DEFENDANT shall conduct an annual regular review of its website and mobile applications to determine the entities with which it makes available PERSONAL INFORMATION. For 2 years from the EFFECTIVE DATE, DEFENDANT shall document and share the results of this review with the People in an annual report, to include the following:

a. The names of entities to which DEFENDANT makes available PERSONAL INFORMATION, the PERSONAL INFORMATION DEFENDANT makes available to these entities, DEFENDANT'S purpose for making PERSONAL INFORMATION available to these entities, and whether DEFENDANT characterizes these entities as SERVICE PROVIDERS.
b. For entities that DEFENDANT contends are SERVICE PROVIDERS, DEFENDANT will enter into contracts with them that meet the requirement of Civil Code section 1798.140, subdivision (v), and document this in the annual report.
c. For entities that are not SERVICE PROVIDERS, SEPHORA shall do any of the following: comply with Civil Code sections 1798.120 and 1798.135; enter into or amend

its contract with the entity to render it a valid SERVICE PROVIDER; or cease making available PERSONAL INFORMATION to that entity.

d. For entities with which DEFENDANT has a specific contractual agreement providing that the entity will act as a SERVICE PROVIDER when processing PERSONAL INFORMATION, but requires the DEFENDANT to enable some type of restricted data processing, DEFENDANT shall enable this restricted data processing for all CONSUMERS, including in its implementation of the Global Privacy Control ("GPC"), or cease making PERSONAL INFORMATION available to the entity.

DEFENDANT shall pay the Attorney General the amount of $1.2 million. The California Attorney General shall deposit said payment into the Consumer Privacy Fund as provided by Civil Code section 1798.155, subdivision (c).

Notes

1. By virtue of their business models, some companies are always going to be first in line for privacy scrutiny. This is the "it is good not to be Facebook" principle in privacy law. Sephora is not normally one of the companies on the front line of the privacy debates. It is a conventional business with a conventional business model. There is nothing in particular that makes it an obvious target for one of the first enforcement actions under the CCPA. On the other hand, it was clearly in violation. Sephora tracked its consumers in the way that all large companies tracked their consumers. It monitored every click of its website and partnered with data analytics firms to better target its products and consumers. All of this counts as the collection of personal data, and all of it was done without attention to CCPA requirements.
2. Consider the size of the fine being issued and the length and intensity of the monitoring program. Is this too much punishment, too little, or just right? There is an obvious similarity to HIPAA's general pattern of settlements. Is that an appropriate model for this case?
3. One of the issues in this case was Sephora's failure to respect Global Privacy Controls (GPCs). GPC is a technical specification that allows Internet users to send a standardized signal to notify websites and services indicating their privacy preferences.[209] Under many state privacy laws, including the CCPA, consumers have a right to limit the sale or sharing of their personal data. It is often impractical for consumers to manually locate and submit their privacy settings on every website, however. GPC is designed to streamline this process by letting consumers make the choice once for all websites.
   GPC is supported by browsers such as Firefox, Brave, and DuckDuckGo. Google Chrome and Safari, two of the most popular browsers, do not currently support GPC directly, however. Those wishing to use GPC on Chrome need to install an extension, such as Privacy Badger.

American Honda Motor Co., No. ENF23-V-HO-2 (Cal. Privacy Prot. Agency, 2025)

STIPULATED FINAL ORDER

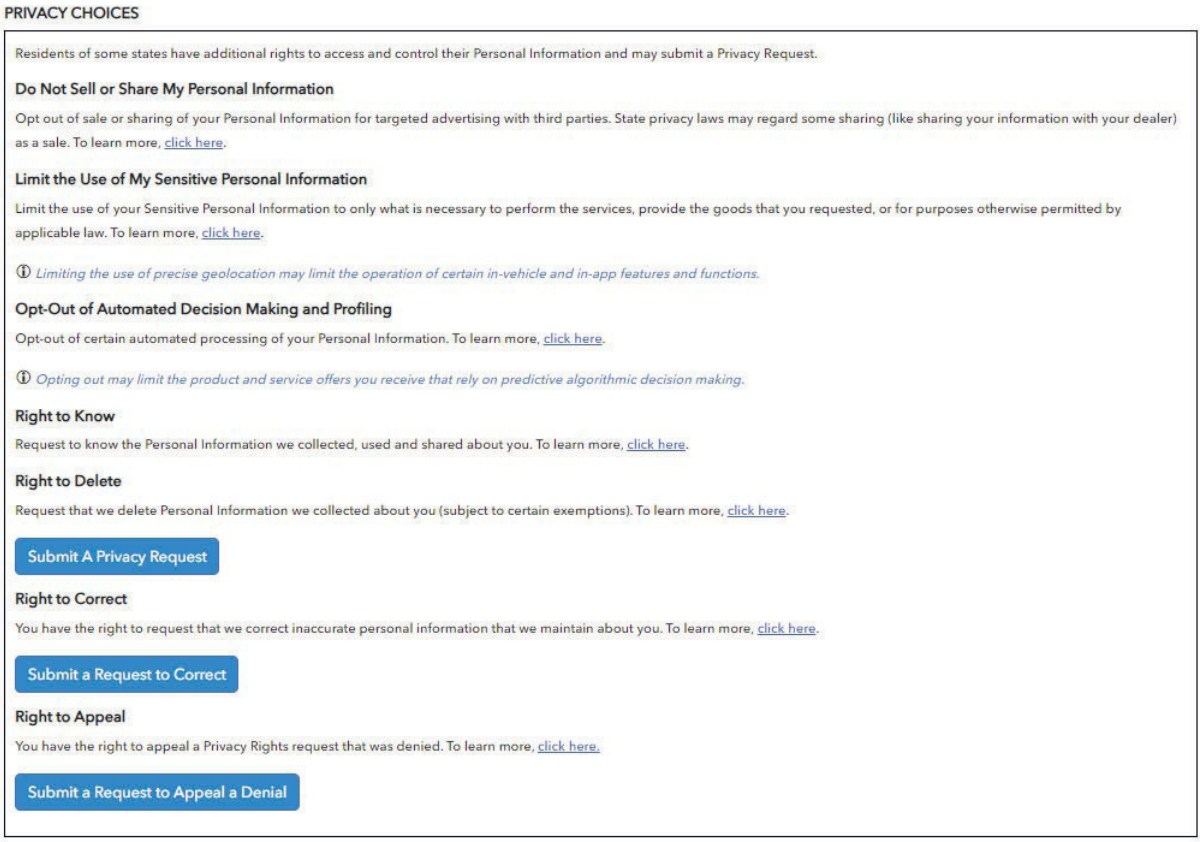
IT IS HEREBY stipulated AND AGREED by and between the parties to the above-entitled matter:

Honda has had a long-standing presence in California going back to its founding in Los Angeles in 1959. Now headquartered in Torrance, California, Honda employs thousands of workers and supplies 126 Honda and 39 Acura automobile dealerships in California.

[209] Global Privacy Control, About, https://globalprivacycontrol.org/#about (last visited June 19, 2025).

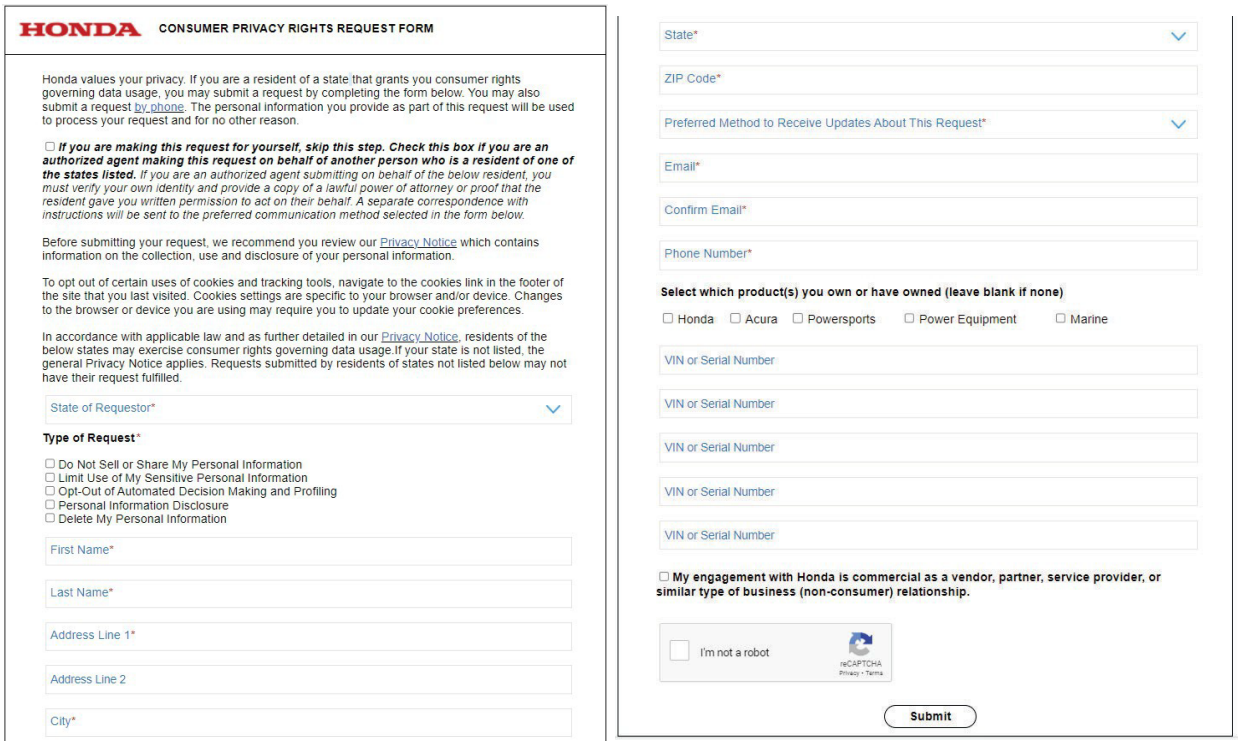
A. Honda's Method for Submitting Requests to Opt-Out of Sale/Sharing and Requests to Limit through its Online Privacy Center

Honda's online Privacy Center includes a listing of privacy choices and links to various requests forms. As shown below, the Privacy Center provides an option for submitting a privacy request, a request to correct, and a request to appeal a denial:



Honda's "Submit a Privacy Request" link takes Consumers to a webform titled "Consumer Privacy Rights Request Form" that requires the same information for five different requests: (1) Do Not Sell of Share My Personal Information, (2) Limit Use of My Sensitive Personal Information, (3) Opt-Out of Automated Decision Making and Profiling, (4) Personal Information Disclosure, and (5) Delete My Personal Information. As shown in the webform below, Honda requires Consumers to provide their first name, last name, address, city, state, zip code, preferred method to receive updates, email, and phone number to submit the request.

Honda also gives Consumers the option to provide the brand of the product they own and the VIN or serial number of their product.



HONDA CONSUMER PRIVACY RIGHTS REQUEST FORM

Honda values your privacy. If you are a resident of a state that grants you consumer rights governing data usage, you may submit a request by completing the form below. You may also submit a request by phone. The personal information you provide as part of this request will be used to process your request and for no other reason.

☐ ***If you are making this request for yourself, skip this step. Check this box if you are an authorized agent making this request on behalf of another person who is a resident of one of the states listed.*** *If you are an authorized agent submitting on behalf of the below resident, you must verify your own identity and provide a copy of a lawful power of attorney or proof that the resident gave you written permission to act on their behalf. A separate correspondence with instructions will be sent to the preferred communication method selected in the form below.*

Before submitting your request, we recommend you review our Privacy Notice which contains information on the collection, use and disclosure of your personal information.

To opt out of certain uses of cookies and tracking tools, navigate to the cookies link in the footer of the site that you last visited. Cookies settings are specific to your browser and/or device. Changes to the browser or device you are using may require you to update your cookie preferences.

In accordance with applicable law and as further detailed in our Privacy Notice, residents of the below states may exercise consumer rights governing data usage.If your state is not listed, the general Privacy Notice applies. Requests submitted by residents of states not listed below may not have their request fulfilled.

State of Requestor*

Type of Request *

☐ Do Not Sell or Share My Personal Information
☐ Limit Use of My Sensitive Personal Information
☐ Opt-Out of Automated Decision Making and Profiling
☐ Personal Information Disclosure
☐ Delete My Personal Information

First Name*

Last Name*

Address Line 1*

Address Line 2

City*

State*

ZIP Code*

Preferred Method to Receive Updates About This Request*

Email*

Confirm Email*

Phone Number*

Select which product(s) you own or have owned (leave blank if none)

☐ Honda ☐ Acura ☐ Powersports ☐ Power Equipment ☐ Marine

VIN or Serial Number

VIN or Serial Number

VIN or Serial Number

VIN or Serial Number

VIN or Serial Number

☐ **My engagement with Honda is commercial as a vendor, partner, service provider, or similar type of business (non-consumer) relationship.**

I'm not a robot reCAPTCHA Privacy - Terms

Submit

By requiring all of this information, Honda's webform unlawfully requires Consumers to provide more information than necessary to exercise their CCPA rights to opt-out of sale/sharing of their personal information and to limit the use and disclosure of their sensitive personal information. Honda essentially applies a verification standard to these rights.

The CCPA distinguishes between Consumer requests that require the business to Verify that the Consumer making the request is the Consumer about whom the business has collected information, and those requests that do not require verification. Specifically, Requests to Delete, Requests to Correct, and Requests to Know are Verifiable Consumer Requests, while Requests to Opt-Out of Sale/Sharing and Requests to Limit are not.

The CCPA regulations governing the submission of Requests to Opt-Out of Sale/Sharing and Requests to Limit are meant to ensure that Consumers can exercise their choices without undue burden. Civ. Code § 1798.185(a)(4). These requests are not verifiable because the potential harm to Consumers resulting from an imposter accessing, deleting, or changing personal information maintained by the business is minimal or nonexistent for Requests to Opt-Out of Sale/Sharing and Requests to Limit.

Accordingly, the CCPA prohibits businesses from requiring Consumers to Verify themselves before processing Requests to Opt-Out of Sale/Sharing and Requests to Limit. At most, businesses may ask Consumers for information necessary to complete the request, such as information necessary to identify the Consumer within their systems, but they may not ask Consumers for more information than necessary to process their requests. To the extent that businesses can comply without additional information, they are required to do so.

From July 1, 2023 through September 23, 2023, Honda required at least 119 Consumers to provide more information than necessary in order to submit their Request to Opt- Out of Sale/Sharing and Request to Limit, and Honda denied at least 20 Consumer requests by unlawfully requiring the Consumer to Verify themselves before processing the request.

B. **Processing Requests to Opt-Out of Sale/Sharing and Requests to Limit Submitted by Consumers' Authorized Agents**

Consumers can authorize other natural persons or business entities, known as Authorized Agents, to act on their behalf in asserting their rights under the CCPA.

Honda's webform for submitting a privacy request contains a checkbox for Authorized Agents who are submitting the request on behalf of a Consumer. Upon checking this box, Honda sends correspondence with instructions to the preferred communication method selected.

The CCPA's prohibition on requiring verification for Requests to Opt-Out of Sale/Sharing and Requests to Limit applies equally to requests submitted by the Consumer's Authorized Agent. Businesses may ask the Consumer's Authorized Agent to provide the Consumer's signed permission demonstrating that they have been authorized to act on the Consumer's behalf. However, businesses may not require the Consumer to directly confirm that they have provided the Authorized Agent permission to submit the request. Businesses may contact Consumers directly in that manner only for Verifiable Consumer Requests.

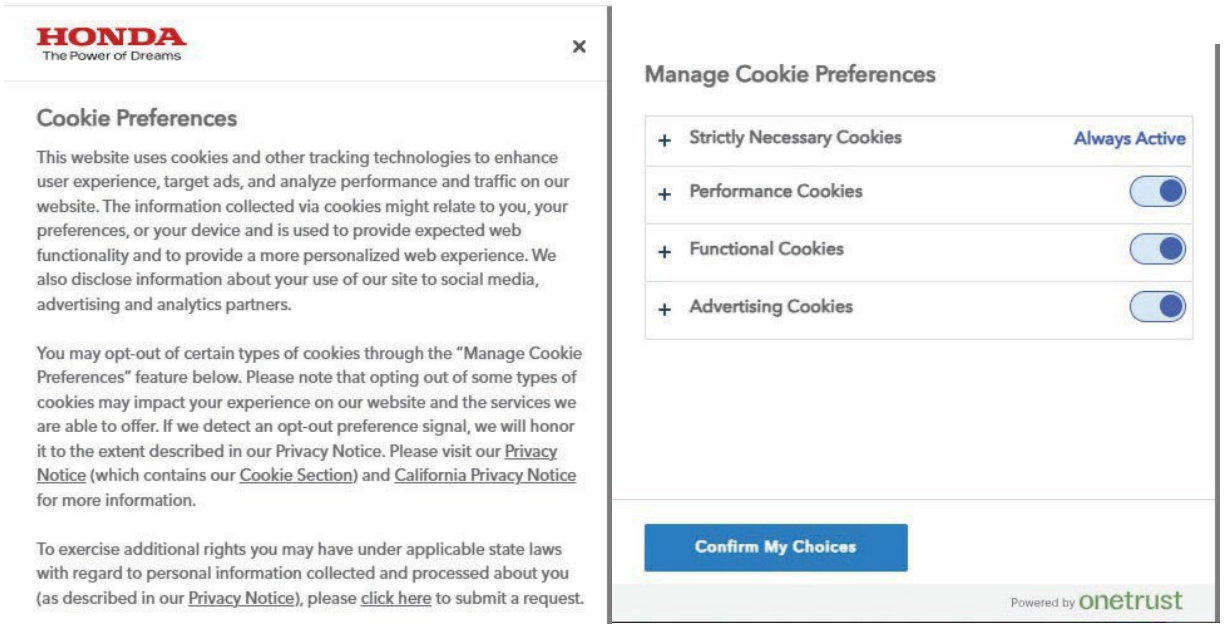
Honda unlawfully requires Consumers to directly confirm with Honda that they had given permission to the Authorized Agent to submit a Request to Opt-Out of Sale/Sharing and Request to Limit.

From July 1, 2023 through September 23, 2023, Honda required at least 14 Consumers to directly confirm with Honda that they had given their Authorized Agents permission to submit the Request to Opt-Out of Sale/Sharing or Request to Limit on their behalf.

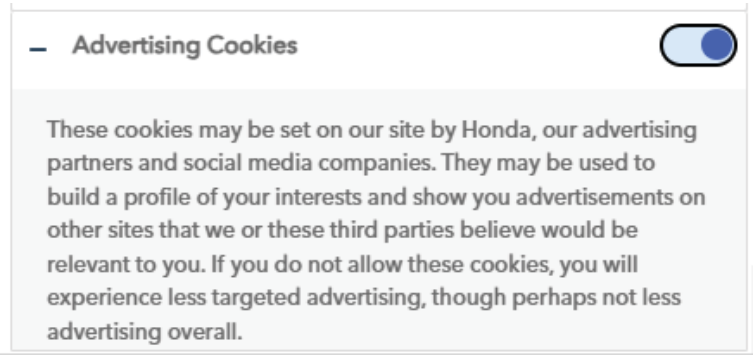
C. Honda's Method for Submitting Requests to Opt-Out of Sale/Sharing through its Cookie Management Tool

Honda contracts with OneTrust, a third-party compliance vendor, to provide a cookie management tool for its Honda and Acura websites. Through the cookie management tool, Consumers can opt-out of advertising and other technology that tracks their activity across different websites for Cross-context Behavioral Advertising purposes.

As demonstrated by the screenshots below, the different types of cookies identified in the cookie management tool (*i.e.*, performance cookies, functional cookies, and advertising cookies) are "allowed" or "active" by default.

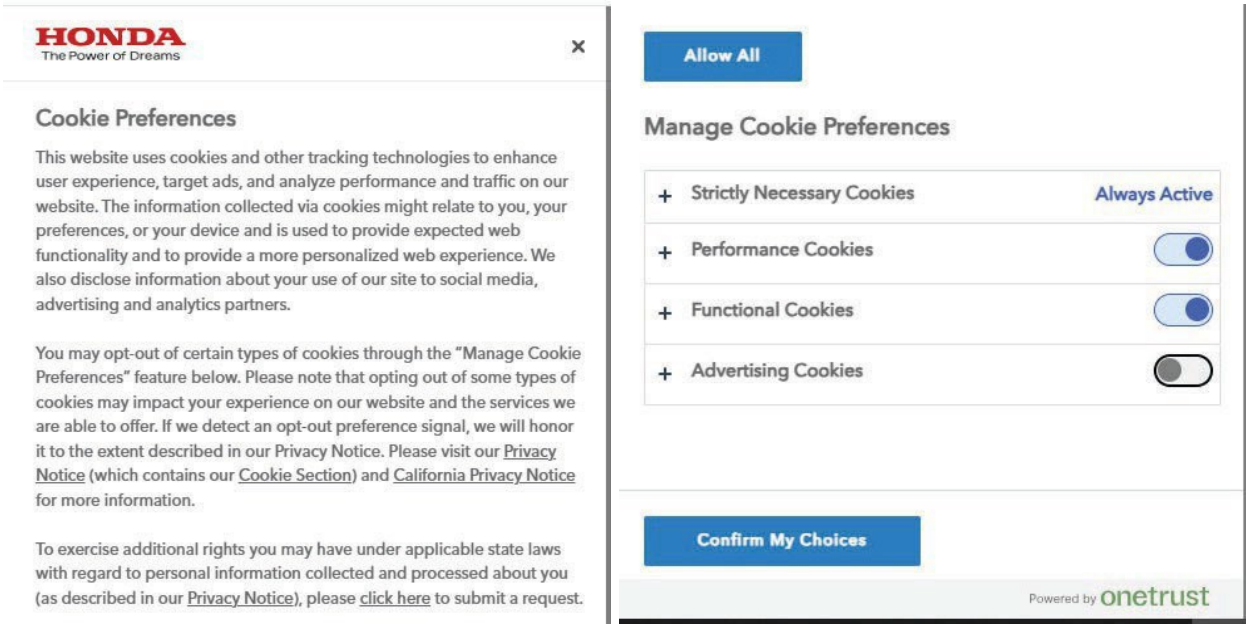


Honda tells Consumers that Advertising Cookies "may be used to build a profile of your interests and show you advertisements on other sites that we or these third parties believe would be relevant to you."



To turn "off" or "disallow" the Advertising Cookies, Consumers must go through two steps. First, they must click on the toggle button to the right of Advertising Cookies, and second, they must click on the "Confirm My Choices" button.

If Consumers return to the cookie management tool after turning "off" the Advertising Cookies, an "Allow All" choice appears.



To opt back into Advertising Cookies, Consumers only need to take one step. By clicking on the "Allow All" button, the cookie management tool will accept the Consumer's choice and the form will disappear.

Businesses must design and implement methods for submitting CCPA requests that are easy to understand, provide symmetry in choice, avoid language or interactive elements that are confusing to the Consumer, avoid choice architecture that impairs or interferes with the Consumer's ability to make a choice, and are easy to execute.

Symmetry in choice means that the path for a Consumer to exercise a more privacy-protection option cannot be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because that would impair or interfere with the Consumer's ability to make a choice.

More specifically, a choice is not symmetrical when a business's process for submitting a Request to Opt-out of Sale/Sharing requires more steps than that business's process for a Consumer to opt-in to the sale of Personal Information after having opted out.

A website banner that provides only two options when seeking Consumers' consent to use their Personal Information—such as "Accept All" and "More Information," or "Accept All" and "Preferences"—is not equal or symmetrical. Such a method is not equal or symmetrical because it allows Consumers to "Accept All" in one step, but requires Consumers to take additional steps to exercise their rights over their Personal Information. An equal or symmetrical choice, by contrast, could be between "Accept All" and "Decline All."

Honda's use of the Advertising Cookies described in its cookie management tool constitutes the Sharing of Personal Information under the CCPA. Honda makes available Consumers' Personal Information to third parties for Cross-Context Behavioral Advertising for which Consumers have the right to opt-out. Accordingly, Honda's cookie management tool is a method through which Consumers can submit their Request to Opt-Out of Sale/Sharing.

Honda's cookie management tool fails to provide symmetrical choice when it comes to Consumers' ability to submit Requests to Opt-Out of Sale/Sharing and for obtaining Consumers' consent to use their Personal Information for the purposes stated in the cookie management tool. While Consumers can "Accept All" cookies with one click, opting out of the cookies requires at least two clicks.

D. Contracts with Advertising Technology Vendors

Honda Collects Personal Information about Consumers on its websites. Honda then Sells, Shares, or discloses that Personal Information to advertising technology companies.

These advertising companies, in turn, use this Personal Information to track Consumers across different websites for advertising and marketing purposes.

The CCPA requires businesses that Collect and disclose Personal Information to a third party, service provider, or a contractor, to enter into an agreement with that third party, service provider, or contractor that meets certain requirements. Those agreements must contain explicit provisions that protect Consumers. For example, the agreements must identify the limited and specified purposes for which the Personal Information can be used and must limit the recipient's use of the Personal Information for only those purposes. The agreements must also require the recipient to comply with the CCPA and provide the same level of privacy protection as required of businesses by the CCPA, among other things.

Despite Collecting, Selling, Sharing, and disclosing Personal Information with these advertising technology companies, Honda could not produce contracts with these advertising technology companies.

IT IS HEREBY ORDERED that:

In accordance with Civil Code § 1798.199.55, Honda shall pay an administrative fine in the amount of six hundred and thirty-two thousand and five hundred dollars ($632,500.00)….

Honda shall modify its methods for submitting CCPA Requests in the following ways. These modifications shall apply to all of Honda's methods for submitting CCPA Requests, such as requests submitted by phone or online, unless otherwise specified.

a) Honda shall only require Consumers making a Request to Opt-Out of Sale/Sharing and Request to Limit to provide information that is necessary to process the request.

b) Honda shall not require Consumers to directly confirm with Honda that they have given their Authorized Agent permission to submit a Request to Opt-Out of Sale/Sharing or Request to Limit on their behalf.

c) Honda shall change its method for submitting Requests to Opt-Out of Sale/Sharing and Requests to Limit by:

    1) For its Privacy Center and online methods for submitting CCPA Requests, separating the methods for submitting Requests to Opt- Out of Sale/Sharing and Requests to Limit from the methods for submitting Verifiable Consumer Requests.
    2) Changing the process for Authorized Agents submitting CCPA Requests so that the Authorized Agents provide their contact information in addition to the Consumer's contact information.
    3) Including the link to manage cookie preferences within its Privacy Center, Privacy Policy, and in the footer of its privacy policy webpages.
    4) Within its cookie management platform, including a "Reject All" button to provide symmetry in choice with Honda's "Allow All" button.
    5) Applying the Global Privacy Control to also apply to known Consumers.

Honda shall consult a user experience (UX) designer, who may be an independent consultant or Honda employee, to evaluate its methods for submitting CCPA Requests and to make recommendations on how to ensure that methods for submitting CCPA Requests are easy to use and avoid language and interactive elements that are confusing to a reasonable Consumer.

Honda shall ensure that all personnel handling CCPA Requests are informed of all requirements under the CCPA…

Honda shall modify its contract management and tracking process to ensure that all required contractual terms are in place…

Notes

1. Think about the power of default options and the power of making those options difficult to change. Under the CCPA people do NOT "Limit Use of My Sensitive Personal Information" or "Opt-Out of Automated Decision Making and Profiling" by default; they must choose to do so. This is a business-friendly design choice. Imagine it were otherwise and people had to affirmatively consent. How many people do you think would opt-in to allowing use of their sensitive personal information?
   But the CCPA then requires that it be easy to opt out of this pro-business default. In fact, the CCPA is willing to tolerate some amount of fraudulent "limit" and "opt-out" requests in service of making it easy to change those settings.
   In general, this kind of thing matters a great deal. Google and Meta care whether 20%, 60%, or 80% of people allow a particular use of their data. Start with a default opt-out and prohibit companies from discriminating against people who do not opt-in, and the number may be closer to 20% for a given setting. Make it default opt-in and difficult to change, and it will be closer to 80%.
2. This case is a window into the world of dark patterns. Dark patterns are user interfaces whose designers knowingly confuse users, make it difficult for users to express their preferences or satisfy their objectives, or manipulate users into taking actions that are inconsistent with their preferences or well-being.[210] Dark patterns typically exploit cognitive biases with the goal of prompting users to purchase goods or services they do not want or surrendering personal information they prefer to keep private. A smartphone app might ask whether a user will authorize push notifications, with the only two response options being "Yes" and "Maybe Later." Then if the user selects "Maybe Later" she will be asked the same question again days later, and again days after that. But once a user clicks on "Yes" they will never be asked to reconsider this choice; this is a "nagging" dark pattern. Alternatively, someone wishing to make a one-time purchase may find themselves subscribing to recurring monthly purchases because that option is selected by default; this is a "preselection" dark pattern. Unappealing aspects of a service may be buried in fine print or a light gray font – an "interface interference" dark pattern. Or opting out of privacy-invasive company practices may needlessly require numerous and time-consuming mouse clicks, an "obstruction" dark pattern.
   Academic data shows that dark patterns occur frequently on websites and that they are incredibly effective at getting people to sign up for unwarranted services or choose privacy-unfriendly settings.[211] Of the first 19 comprehensive state privacy laws, 13 define "consent" for at least some purposes as consent obtained free from dark patterns or mechanisms that impair user autonomy.[212] This is a growing area of law, and likely to be a major issue in privacy class action litigation in years to come.

---

[210] Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANAL. 43 (2021); Colin M. Gray, Cristiana Santos, Nataliia Bielova & Thomas Mildner, *An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building*, in ' CHI 24: PROCEEDINGS OF THE 2024 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (May 2024), available at https://dl.acm.org/doi/10.1145/3613904.3642436; *see also* Cal. Priv. Prot. Agency, CAL. CODE REGS. TIT. 11, § 7004(c) (2023) ("A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice.").

[211] For a review, see Matthew B. Kugler, Lior Strahilevitz, Marshini Chetty, Chirag Mahapatra & Yaretzi Ulloa, *Can Consumers Protect Themselves Against Privacy Dark Patterns?* 23 U.N.H. L. REV. (forthcoming, 2025).

[212] See *id*. at *8–9.

3. In 2026, California settled with General Motors (GM) in another automotive privacy case. According to the complaint, GM collected extensive location data through its linked OnStar services and sold this data to brokers despite implying that it would only be used to deliver requested services. The retention of this data also allegedly violated the purpose and data minimization requirements of the CCPA. GM agreed to wide-ranging reforms, including a prohibition on selling such data, and a 12.75 million dollar fine.[213] This case shows California's continued interest in automotive privacy and location data. The case is also notable for a comment made regarding consumer harm. Though the data brokers used the information to generate risk scores for auto insurance pricing, California insurers were actually prohibited from using driving data to set prices. So Californian consumers, unlike consumers in other states, did not see insurance pricing effects from GM's data sales.

California Delete Act

Though not a comprehensive privacy law, the California Delete Act is another state provision with wide-ranging implications. The California Delete Act (SB 362) was enacted on October 10, 2023. The Act regulates data brokers, defined as "business[es] that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship," with certain carve-outs for entities covered by other statutory regimes. A "direct relationship" is defined as one in which "a consumer intentionally interacts with a business for the purpose of obtaining information about, accessing, purchasing, using, or requesting the business's products or services within the preceding three years." Cal. Code Regs. tit. 11, § 7601 (2025).

The Delete Act transferred the data broker registry from the Attorney General's office to the California Privacy Protection Agency (CPPA). Starting January 1, 2024, data brokers face a daily fine of $200 for not registering. Upon registration, data brokers must disclose whether they collect personal information of minors, precise geolocation data, or reproductive health data, and whether they are covered by other statutory regimes such as HIPAA.

In addition to the registry, the Delete Act mandates the California Privacy Protection Agency (CPPA) to implement a Delete Request and Opt-Out Platform (DROP) by January 1, 2026. Cal. Civ. Code § 1798.99.86 (West 2025) The Platform, funded by the data broker registration fees, gives California consumers a unified interface to submit free deletion requests, verify their identity to data brokers, select specific data brokers for deletion, and modify prior deletion requests.

Beginning August 1, 2026, data brokers have 45 days to process such a request; they must either delete the consumer's information or, if the request cannot be verified, treat it as an opt-out of sale. The deletion request is revolving: after deleting the consumer's data, the data broker must continue to delete their personal information at least once every 45 days and may not sell or share their information.

The Delete Act also imposes annual disclosure obligations on data brokers. In each calendar year, data brokers must disclose the number of deletion requests received, complied with (in whole or in part) and denied (in whole or in part and the basis for denial), their response time data, and the number of denied requests categorized by reason.[214]

---

[213] Cal. Priv. Prot. Agency, *When It Comes to Data Privacy, Consumers Must Be in the Driver's Seat: Attorney General Bonta, Partners Secure $12.75 Million General Motors Privacy Settlement* (May 8, 2026), https://privacy.ca.gov/2026/05/when-it-comes-to-data-privacy-consumers-must-be-in-the-drivers-seat-attorney-general-bonta-partners-secure-12-75-million-general-motors-privacy-settlement/

[214] Cal. Civ. Code § 1798.99.85 (West 2025), *see also* Ken D. Kumayama et al., *California's Data Deletion Law Imposes a Host of New Obligations on Data Brokers*, SKADDEN (Dec. 14, 2023), https://www.skadden.com/insights/publications/2023/12/californias-new-data-deletion-law-imposes.

Finally, the Delete Act requires data brokers to submit to an independent third-party privacy audit beginning on January 1, 2028 every 3 years, and submit the audit report to the CPPA upon request.

Following an investigative sweep in late 2024, the CPPA initiated several enforcement actions, including fines against five data brokers that failed to register.[215] The current data broker registry is available on CPPA's website, and the agency is seeking information on data brokers that fail to register.[216]

By January 2025, CPPA had reached settlements with five data brokers that failed to register.[217] Due to the daily fine structure, the penalties were relatively modest—typically in the tens of thousands of dollars.[218] One particular settlement with Background Alert, Inc. stands out. Background Alert, Inc. was found to have failed to register between February and October 2024. As part of its settlement, the company agreed to shut down operations through 2028 or face a $50,000 fine.[219] While the monetary value is still modest, the operational shutdown is unique among the settlements.

Notes

1. Imagine you have the ability to submit a delete request under the California Delete Act. Would you do so? Is there any good reason *not* to do so? Would it be bad for society if *everyone* did so, and thus the entire data broker industry was destroyed? In one study of dark patterns, users were given the option to turn on a "do not sell or share my personal information" setting during the signup process for a fake video streaming website. In the control condition, over 70% of people turned that setting on.[220] Does that mean that we should default to having people opted-out of such sharing, since that is what most people want?
2. The Delete Act remains "in progress" during the 2026-2027 academic year. During Spring 2026, an analysis of data broker website suggests that there is only partial compliance with the then-existing Delete Act and relevant CCPA requirements.[221] Some data brokers were found to have made it impossible for consumers to fully exercise their rights and some to have introduced meaningful barriers to them doing so. The authors attribute this incomplete compliance to the lack of a private right of action and lack of clear financial penalties for some forms of noncompliance.

2) Other states

A number of other states followed California's lead in the early 2020s. As of the start of 2024, comprehensive privacy laws are in effect in Colorado, Connecticut, Virginia, and Utah.

---

[215] California Privacy Protection Agency, *CPPA's Enforcement Division Inks Settlement with Fifth Data Broker* (Jan. 29, 2025), https://cppa.ca.gov/announcements/2025/20250129.html.

[216] *See* California Privacy Protection Agency, *Data Broker Registry*, https://cppa.ca.gov/data_broker_registry/ (last visited June 8, 2025).

[217] Cal. Privacy Prot. Agency, *CPPA's Enforcement Division Inks Settlement with Fifth Data Broker* (Jan. 29, 2025), https://cppa.ca.gov/announcements/2025/20250129.html.

[218] *Id.*; *see also* California Privacy Protection Agency, *CPPA Brings Enforcement Action Against Florida Data Broker* (Feb. 20, 2025), https://cppa.ca.gov/announcements/2025/20250220.html.

[219] Cal. Privacy Prot. Agency, *Data Broker Promoting Ability to Dig Up "Scary" Amounts of Information Agrees to Shut Down* (Feb. 27, 2025), https://cppa.ca.gov/announcements/2025/20250227.html.

[220] Se Matthew B. Kugler, Lior Strahilevitz, Marshini Chetty, Chirag Mahapatra & Yaretzi Ulloa, *Can Consumers Protect Themselves Against Privacy Dark Patterns?* 23 U.N.H. L. REV. (forthcoming, 2025).

[221] Anna-Maria Gueorguieva, Jennifer King, Apoorva Panidapu & Daniel E. Ho, *Privacy Without Remedy: An Assessment of Data Broker Compliance with California Privacy Law*, in The 2026 ACM Conference on Fairness, Accountability, and Transparency (FAccT '26) (2026), https://doi.org/10.1145/3805689.3812413

Laws have been passed and are expected to go into effect over the next several years in Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, and Texas.

It is neither possible nor desirable to comprehensively review each of these laws. If one traces how any particular issue is handled across the statutes, however, it rapidly becomes clear that every state is working off a similar template. The details of that template's implementation vary sharply across states, but the general form is consistent.

Scope. These laws do not have universal application. As with California, they tend to limit their scope to include only entities of a particular size and type. A state might restrict its privacy statute to apply only to entities that process data on a certain number of state residents or derive a certain portion of their revenue from the sale of personal data. The law might further exclude from consideration certain industries, such as those regulated by Gramm–Leach–Bliley or HIPAA. It might even specifically exclude nonprofits.

The Connecticut statute, for instance, covers entities that

> (1) Controlled or processed the personal data of not fewer than thirty-five thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
>
> (2) control or process consumers' sensitive data, excluding personal data controlled or processed solely for the purposes of completing a payment transaction; or
>
> (3) offer consumers' personal data for sale in trade or commerce.

CONN. GEN. STAT. § 42-516. The statute then excludes from its coverage any state entity, nonprofit, institute of higher education, HIPAA-covered entity, or financial institution covered under either the Securities and Exchange Act or Gramm–Leach–Bliley Act. CONN. GEN. STAT. § 42-517(a). The Virginia statute's scope is similar, requiring either data on 100,000 consumers or data on 25,000 consumers while also deriving 50% of gross revenue from the sale of personal data. VA. CODE § 59.1-576(A). The list of exempt entities in Virginia is almost identical to the one in Connecticut. VA. CODE § 59.1-576 (B).

Personal Data and Publicly Available Data. Both statutes define personal data as data that can be linked to an identifiable individual and excludes from the definition publicly available data. Consider CONN. GEN. STAT. § 42-515:

> (27) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.
>
> (34) "Publicly available information"
>
> (A) means information that
>
> (i) is lawfully made available from federal, state or municipal government records, or
>
> (ii) a controller has a reasonable basis to believe (I) a consumer has lawfully made available to the general public, or (II) has been lawfully made available to the general public from widely distributed media, and
>
> (B) does not include any biometric data that can be associated with a specific consumer and were collected without the consumer's consent.

Yet there can be important nuances. Consider the definition in Virginia:

> "Publicly available information" means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, *unless the consumer has restricted the information to a specific audience.* (emphasis added). VA. CODE § 59.1-575.

Sensitive Data. All of these states create a category of sensitive personal data and give residents enhanced rights over the processing of this data. Almost every state requires that an entity either have the consent of the data subject to process the data or a need to process the data to provide the data subject with a product or service that they have requested. Two states—Iowa and Utah—instead require that residents receive notice and be given the opportunity to opt out.

Connecticut is one of the states that requires consent to process sensitive data. CONN. GEN. STAT. § 42-520(a). It defines sensitive data as

> personal data that includes
>
> (A) data revealing (i) racial or ethnic origin, (ii) religious beliefs, (iii) a mental or physical health condition, diagnosis, disability or treatment, (iv) sex life, sexual orientation or status as nonbinary or transgender, or (v) citizenship or immigration status,
>
> (B) consumer health data,
>
> (C) genetic or biometric data or information derived therefrom,
>
> (D) personal data collected from an individual the controller has actual knowledge, or willfully disregards, is a child,
>
> (E) data concerning an individual's status as a victim of crime, as defined in section 1-1k, (F) precise geolocation data,
>
> (G) neural data,
>
> (H) a consumer's financial account number, financial account log-in information or credit card or debit card number that, in combination with any required access or security code, password or credential, would allow access to a consumer's financial account, or
>
> (I) government-issued identification number, including, but not limited to, Social Security number, passport number, state identification card number or driver's license number, that applicable law does not require to be publicly displayed.CONN. GEN. STAT. § 42-515.

Consumer Rights. These statutes give consumers a fairly standard set of rights. These rights are generally somewhat more limited than those granted under the CCPA, but share common themes. For instance, here are the rights granted under Connecticut's law. Consumers have the right to:

> (1) Confirm whether or not a controller is processing the consumer's personal data and access such personal data, including, but not limited to, any inferences about the consumer derived from such personal data and whether a controller or processor is processing a consumer's personal data for the purposes of profiling to make a decision that produces any legal or similarly significant effect concerning a consumer, unless such confirmation or access would require the

> controller to reveal a trade secret or the controller is prohibited from disclosing such personal data under subsection (e) of this section;
>
> (2) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;
>
> (3) delete personal data provided by, or obtained about, the consumer;
>
> (4) obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret; and
>
> (5) opt out of the processing of the personal data for purposes of (A) targeted advertising, (B) the sale of personal data, except as provided in subsection (b) of section 6 of this act, or (C) profiling in furtherance of any automated decision that produces any legal or similarly significant [effects] effect concerning the consumer….
>
> (7) obtain from the controller a list of the third parties to which such controller has sold the consumer's personal data or, if such controller does not maintain a list of the third parties to which such controller has sold the consumer's personal data, a list of all third parties to which such controller has sold personal data, provided the controller shall not be required to reveal any trade secret.

CONN. GEN. STAT. § 42-518. Further, a covered entity shall:

> (A) Limit the collection of personal data to what is reasonably necessary and proportionate in relation to the purposes for which such data are processed, as disclosed to the consumer;
>
> (B) unless the controller obtains the consumer's consent, not process the consumer's personal data for any material new purpose that is neither reasonably necessary to, nor compatible with, the purposes that were disclosed to the consumer … taking into account [various factors, including the consumer's reasonable expectations, the relationship between consumer and entity, and safeguards]
>
> (C) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue;
>
> (D) not process sensitive data concerning a consumer unless such processing is reasonably necessary in relation to the purposes for which such sensitive data are processed and without obtaining the consumer's consent…
>
> (G) provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent….
>
> (H) not sell the sensitive data of a consumer without the consumer's consent…

CONN. GEN. STAT. § 42-520. If the entity sells personal data to third parties or processes data for targeted advertising, the entity must disclose this and give the consumer an opportunity to opt out. Virginia law is similar, though not as expansive as this amended text. VA. CODE §§ 59.1-577–578.

Enforcement. All of these states have thus far opted for state agency enforcement rather than provide a private right of action. Penalties available to public enforcers vary. The Connecticut statute allows for penalties up to $5,000 per violation under the Connecticut Unfair Trade Practices Act. CONN. GEN. STAT. § 42-525. The Virginia statute authorizes penalties of up to $7,500 per violation. VA. CODE § 59.1-584.

Cure. States sometimes give covered entities the opportunity to repair violations before the state can file an enforcement action against them. Connecticut had a mandatory cure/waiting period on enforcement actions up until December 31, 2024, and then an optional cure/waiting period after that. CON. PUB. ACT 22-15 § 11. Virginia has a mandatory 30-day cure period, which is triggered only when the Attorney General notifies the entity of the specific provisions it believes the entity is violating. VA. CODE § 59.1-584.

X. Data Security

A. Data Breach Notification Laws 551

B. Data Breach Lawsuits.....554
Tsao v. Captiva MVP Restaurant Partners, LLC, 986 F.3d 1332 (11th Cir. 2021) 554
In re Equifax, Inc., Customer Data Security Breach Litig., 362 F.Supp.3d 1295 (N.D. Ga. 2019) 562

C. Federal Trade Commission and Data Security.....571
FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015) 573
LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018) 579
In the Matter of Chegg, Inc. (FTC 2023) 585

It is helpful to distinguish between data privacy and data security. Data privacy is about whether your data does what you want it to. Data security is about whether your data does what Facebook wants it to do. Are only people authorized by Facebook able to access the data you post to Facebook, or are other people accessing it as well?

In general, then, companies sometimes want to have bad data privacy—they want the freedom to use data however they like even if their customers have other preferences. But it is a rare company that wants to have bad data security; companies would prefer more control rather than less over their data. So why do so many companies seem to have bad data security? Why are there so many hacks? One reason is that data security does not generate revenue. A marketing department can claim that an additional X% of budget will lead to Y% of increased sales, but data security employees cannot do the same. Data security is generally about stopping bad things from happening—hacks, bad press, large fines—and not making good things happen. Though "losses loom larger than gains" in individual decision-making, this does not appear to translate to corporate budgeting. So, companies are systematically incentivized to underinvest in data security.

A further reason why companies may underinvest in data security is the connection between security and friction. Most data security measures slow things down. Passwords get longer and more unique; people get prompted to pull out their phone for two-factor authentication; supervisors get paged to grant subordinates access to high-level files and systems. Each of these points of friction is costly. Employees are slower and customers may become frustrated in their efforts to spend money.

A. Data Breach Notification Laws

The first major portion of data security law is a series of statutes that require companies to notify individuals when data concerning those individuals is breached. California passed the nation's first data breach notification law in 2002. Following the ChoicePoint data breach of 2005, where the personal financial records of more than 163,000 consumers were compromised, many other states followed suit. By the end of 2006, 33 states had passed their own data breach laws. Today, all 50 states, D.C., Guam, Puerto Rico, and the Virgin Islands have their own data breach laws.

With every state having its own data breach law, one might think this would be a natural opportunity for federal harmonizing legislation. This has not occurred. Though some sectoral federal statutes have their own data breach notification requirements (HIPAA, for instance), there is no general federal data breach law.

The state laws themselves contain important differences. Several law firms and the International Association of Privacy Professionals have publicly available documents that collect, summarize, and attempt to sort the various state data breach laws. Imagine you are general counsel of a major national company that has experienced a data breach affecting individuals in all 50 states. Let us be kind and assume that you do not have customers in D.C., Puerto Rico, Guam or the U.S. Virgin Islands. Foley & Lardner has an 80-page PDF summarizing the laws that have suddenly become relevant to your business.[222] That PDF opens with a description of all the information that is not contained within it, such as what it means to notify people. If you think this sounds like a compliance nightmare, you would be correct.

Despite the variation in state statutes, there is also much commonality. Let us look at California's statute, CAL. CIV. CODE § 1798.82. Due to its first-mover status, California served as a model for many other states.

Application. The data breach law covers any person, business, or state agency that does business in California and owns or licenses computer data containing personal information. Such an entity "shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" along with the encryption key required to make it readable.

Personal information. Personal information means either a username or email address, in combination with a password or security question and answer that would permit access to an online account, or "[a]n individual's first name or first initial and last name" in combination with any of the following:

A. Social security number.
B. Driver's license number or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
C. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
D. Medical information.
E. Health insurance information.
F. Unique biometric data, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
G. Information or data collected through the use or operation of an automated license plate recognition system.
H. Genetic data.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Definition of breach. A breach is the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further

[222] Jennifer Urban, Jennifer Hennessy, & Samuel Goldstick, *State Data Breach Notification Laws,* FOLEY & LARDNER LLP (July 9, 2024), https://www.foley.com/insights/publications/2024/04/state-data-breach-notification-laws/.

unauthorized disclosure." Information that is only breached in encrypted form does not count as having been compromised unless the encryption key is also obtained.

Notice to individuals. The notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present [information] under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." There are more detailed requirements about what must be included under each of those categories.

Notice to the state. If a single breach has affected more than 500 California residents, a copy of the notification must be submitted to the Attorney General.

Timing. "The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."

Enforcement. Individuals can bring a civil action against a company for its failure to abide by the notification provisions, but there are no statutory damages.

Other states vary on each of these points. Michigan, for instance, does not require notification if the entity determines that the breach has not or is not likely to cause substantial loss, injury, or identity theft to one or more Michigan residents, MICH. COMP. LAWS § 445.72, and Colorado is similar, COLO. REV. STAT. § 6-1-716. Georgia's definition of personal information does not mention biometrics, health information or health insurance information, or genetics. GA. CODE ANN. § 10-1-910. Texas requires notice to the state if more than 250 Texas residents are affected, TEX. BUS. & COM. CODE § 521.002; New York requires notice to three separate state actors if *any* New York resident is affected, N.Y. GEN. BUS. L. § 899-aa; and Wyoming never requires notice to the state, WYO. STAT. ANN. §§ 40-12-502. The exact form of the notice also varies from state to state, and states have complicated procedures regarding when notice can be made electronically versus by mail (mail obviously being quite costly at scale). Oh, and states sometimes have content-specific data breach statutes. For instance, California has a medical information data breach statute that adds additional protections.[223]

One other major distinguishing factor is the trigger for notification. California requires that the data be "acquired" by an unauthorized party. Acquisition may mean "in the physical possession and control of an unauthorized person" or "has been downloaded or copied" or "was used by an unauthorized person." In contrast, some states require only that the data have been "accessed" by unauthorized individuals. CONN. GEN. STAT. § 36a-701b; N.J. STAT. ANN. §§ 56:8-161; N.Y. GEN. BUS. L. § 899-aa. These statutes would apply if unauthorized people looked at data without copying it. Frequently, all that can be known is that a hacker broke in and improperly accessed the data; whether the hacker copied it or used it is unknown.

When a data breach occurs, the initial task of the affected company or agency is to investigate the breach and figure out what happened—whose data was exposed, what data was exposed for each person, was the data copied or merely viewed, which state laws apply, etc. Whether it is the company's fault that it was breached is actually not very relevant to the notification analysis. Data breach notification is, in that sense, strict liability.

The general theory of data breach notification is that it allows individual to engage in self-help. Upon receiving a data breach notification, people can change passwords, cancel credit cards, and begin monitoring their credentials for unauthorized lines of credit. In practice, there is reason to think that most people do not do this. This has led some to argue that the massive amount of resources companies spend notifying people of data breaches could be better spent

[223] All of this is independent of and in addition to the California Consumer Privacy Act, which has its own data security provisions.

on actually improving data security. Others counter that the cost and embarrassment of sending out data breach notifications incentivizes companies to avoid being breached in the first place.

It is also important to remember that there are non-statutory data security obligations. If a store that accepts Visa realizes that it has experienced a data breach, the store must abide by its contract with Visa in addition to state data breach laws. This contract will almost certainly require that the store swiftly notify Visa even if the breach is not reportable under state statute.

B. Data Breach Lawsuits

Few seriously question the proposition that data breaches cause harm. If a company mishandles payment information and exposes the credit card numbers of 10,000 customers, some of those customers will likely experience fraudulent charges. But it turns out that it is sometimes hard to localize the resultant harm. In general, people in the United States are not liable for fraudulent credit card charges if they promptly report them; most credit cards refund such charges after an investigation. So, the most basic form of harm—direct financial loss from fraud—tends to be displaced from the person whose information was stolen to the credit card company, which in turn will generally displace it still further onto the merchant who accepted the fraudulent transaction. But there are other theories of harm. For example, people have claimed: emotional injury from having their information exposed; increased risk of future harm, especially when the information exposed is permanent, as in the case of social security numbers; cost of precautions to reduce the risk of future harm/identity theft; and sorting out costs (the time spent dealing with all the above).

Courts have sometimes been resistant to recognizing some of these categories of harm. This resistance sometimes comes in the form of dismissal for lack of Article III standing, as shown in *Tsao*, below.

Tsao v. Captiva MVP Restaurant Partners, LLC, 986 F.3d 1332 (11th Cir. 2021)

TJOFLAT, Circuit Judge:

Tsao seeks to bring a number of claims against PDQ—a restaurant he patroned—following a data breach that exposed PDQ customers' personal financial information. Tsao's appeal presents two questions. First, did Tsao have standing to sue based on the theory that he and a proposed class of PDQ customers are now exposed to a substantial risk of future identity theft, even though neither Tsao nor the class members have suffered any misuse of their information? Second, and alternatively, were Tsao's efforts to mitigate the risk of future identity theft a present, concrete injury sufficient to confer standing? For both questions, we conclude the answer is no . . . .

PDQ is a group of fast casual restaurants that sells chicken tenders, chicken nuggets, salads, and sandwiches. Like most restaurants today, PDQ accepts payment through a point-of-sale system where customers can insert credit or debit cards to pay for their meal. When customers pay with a debit or credit card, PDQ collects some data from the cards, including the cardholder's name, the account number, the card's expiration date, the card verification value code ("CVV"), and PIN data for debit cards. PDQ then stores this data in its point-of-sale system and transmits the information to a third party for processing and for completion of the payment.

Beginning on May 19, 2017, a hacker exploited PDQ's point of sale system and gained access to customers' personal data—the credit and debit card information—through an outside vendor's remote connection tool. PDQ later became aware of the breach, and on June 22, 2018, it posted a notice to customers that it had "been the target of a cyber-attack." The notice stated

that "[a]ll PDQ locations in operation" between May 19, 2017, and April 20, 2018, were affected by the attack, and the notice listed the customers' personal information that "may have been accessed": cardholder names, credit card numbers, card expiration dates, and CVVs. Because of the nature of the breach, PDQ stated that it "was not possible to determine the identity or exact number of credit card numbers or names that were accessed or acquired during" the cyber-attack. The notice repeatedly made clear that PDQ customers' information "may" have been accessed.

In October 2017—during the data breach period—plaintiff Tsao made at least two food purchases at a PDQ restaurant in Pinellas, Florida, using two different cards. Both of these cards offer Tsao the ability to accrue points or rebates by making certain types of purchases—gas, dining, groceries, and travel, just to name a few. Because Tsao made purchases at PDQ during the breach period, the credit card data from these cards may have been accessed by hackers. So, when Tsao learned of the possible breach in 2018, he contacted both Chase and Wells Fargo and cancelled his cards.

Less than two weeks after PDQ's announcement of the cyber-attack, Tsao filed a class action complaint in the Middle District of Florida on behalf of a nationwide class, or alternatively, a separate Florida class. The Complaint lists a variety of injuries that PDQ customers allegedly suffered as a result of the cyber-attack, including "theft of their personal financial information," "unauthorized charges on their debit and credit card accounts," and "ascertainable losses in the form of the loss of cash back or other benefits." Tsao asserts that he and the class members "have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives."

Based on these alleged injuries, the Complaint claims that PDQ (1) breached an implied contract by failing to safeguard customers' credit card data (Count I); (2) was negligent in failing to provide adequate security for the credit card data (Count II); (3) was *per se* negligent because PDQ violated Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), which prohibits unfair practices that affect commerce (Count III); (4) was unjustly enriched when it received payments from the customers but failed to provide those customers with adequate data security (Count IV); and (5) violated the Florida Unfair and Deceptive Trade Practices Act by failing to, among other things, maintain "adequate . . . data security practices" (Count VI). The Complaint additionally seeks a declaratory judgment stating that "PDQ's existing data security measures do not comply with its contractual obligations and duties of care" and that PDQ, in order to comply with those obligations, is required to implement and maintain a variety of security measures (Count V).

PDQ moved to dismiss the Complaint on August 28, 2018. PDQ argued that the Complaint failed to state a claim [and lacked standing]. On the standing issue, PDQ emphasized that, although customer data may have been "compromised" or "exposed" during the cyber-attack, Tsao failed to identify "a single incident involving an actual misuse of the credit card information, much less any misuse . . . causing any of the customers any *actual injury*" (emphasis in original). Instead, PDQ argued, Tsao's claims were "premised on a fear that his credit card information may be misused at some point in the future," and since he cancelled his cards before any misuse occurred, he was foreclosed from alleging damages. And even if Tsao did incur some out-of-pocket expenses to mitigate the risk of misuse, PDQ claimed that such "manufacture[d] standing" was not enough to satisfy Article III.

Tsao's response to the motion to dismiss focused heavily on three types of injuries he allegedly suffered in his efforts to mitigate the perceived risk of future identity theft: lost cash back or reward points, lost time spent addressing the problems caused by the cyber-attack, and restricted card access resulting from his credit card cancellations. [T]he thrust of Tsao's response was that he had standing (1) because he and the class were at an elevated risk of

identity theft, or, alternatively, (2) because he took "proactive[]" steps to mitigate the risk of identity theft.

On November 1, 2018, the District Court dismissed Tsao's Complaint without prejudice for lack of standing. This appeal followed.

Tsao's arguments focus on two general theories of standing. First, he argues that he *could* suffer future injury from misuse of the personal information disclosed during the cyber-attack (though he has not yet), and this risk of misuse alone is enough to satisfy the standing requirement. Then, he argues that he has *already* suffered some "concrete, particularized" mitigation injuries—for example, lost time, lost rewards points, and loss of access to accounts—that are sufficient to confer standing.

Under Article III of the Constitution, the jurisdiction of a federal court is limited to "cases" and "controversies." To satisfy the "case" or "controversy" requirement, a plaintiff in a matter must have standing to sue. And for a plaintiff to have standing, it must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision."

Of the three standing elements, Tsao's allegations implicate only injury. At the pleading stage, "general factual allegations of injury" are enough. *Lujan v. Defs. of Wildlife* (1992). But this does not mean that *any* allegations of injury can push a plaintiff across the standing threshold. Rather, a plaintiff must set forth general factual allegations that "plausibly and clearly allege a concrete injury," and that injury must be "'actual or imminent, not conjectural or hypothetical.'" "[M]ere conclusory statements[] do not suffice."

This standing framework raises two questions. First, what is a "concrete" injury? In *Spokeo, Inc. v. Robins* (2016), the United States Supreme Court offered a straightforward definition: "A concrete injury must be *de facto*; that is, it must actually exist." The Supreme Court noted that, when it uses the term "concrete," it intends to "convey the usual meaning of the term—'real,' and not 'abstract.'"

Typically, tangible[1] injuries are "concrete." Tangible injuries can include both straightforward economic injuries and more nebulous injuries, like lost time or the loss of a "fraction of a vote."

But although many types of injuries may qualify as "concrete," there is another restriction on standing: "Where a 'hypothetical future harm' is not 'certainly impending,' plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves.'" This raises the second question: When is an injury "actual or imminent" and not just "conjectural or hypothetical?"

[W]e can distill two legal principles relevant to Tsao's claims. First, a plaintiff alleging a threat of harm does not have Article III standing unless the hypothetical harm alleged is either "certainly impending" or there is a "substantial risk" of such harm.[2] *Clapper v. Amnesty Int'l USA* (2013). Second, if the hypothetical harm alleged is not "certainly impending," or if there is not a substantial risk of the harm, a plaintiff cannot conjure standing by inflicting some direct harm on itself to mitigate a perceived risk. With these two principles in mind, we turn to Tsao's claims.

We begin with Tsao's theory that he has Article III standing because he faces a "substantial risk of identity theft, fraud, and other harm in the future as a result of the data breach." Although this Circuit has not addressed the issue head-on, a number of our sister

---

[1] Intangible injuries, such as a mere statutory violation, will sometimes qualify as concrete, but that inquiry depends upon the context of the statutory violation.

[2] The Supreme Court indicated that both the "certainly impending" and "substantial risk" standards are applicable in future injury cases, albeit without resolving whether they are distinct.

circuits have, and they are divided. On the one hand, the Sixth, Seventh, Ninth, and D.C. Circuits have all recognized—at the pleading stage—that a plaintiff can establish injury-in-fact based on the increased risk of identity theft. On the other hand, the Second, Third, Fourth, and Eighth Circuits have declined to find standing on that theory.[3]

Generally speaking, the cases conferring standing after a data breach based on an increased risk of theft or misuse included at least some allegations of actual misuse or actual access to personal data. In *Attias v. Carefirst, Inc.* (D.C. Cir. 2017), two plaintiffs alleged that they suffered identity theft when their anticipated tax refunds went missing. In *Galaria v. Nationwide Mut. Ins. Co.* (6th Cir. 2016), plaintiffs alleged that their data was accessed and had "already been stolen" by "ill-intentioned criminals." In *Remijas v. Neiman Marcus Grp., LLC* (7th Cir. 2015), plaintiffs alleged that personal data had "already been stolen" and that "9,200 cards [] experienced fraudulent charges." And in *Krottner v. Starbucks Corp.* (9th Cir. 2010), at least one plaintiff alleged that someone "attempted to open a bank account in his name."

Other Circuits have declined to find standing on an "elevated risk of identity theft" theory where the plaintiffs failed to allege any actual misuse of class members' personal information. The Second Circuit, for example, distinguished a breach of credit-card-specific data from a breach of other forms of personal information in *Whalen v. Michaels Stores, Inc* (2d Cir. 2017). In *Whalen*, Michaels Stores publicly announced a breach of card data, and Whalen filed suit alleging that her card—which was used at Michaels during the breach period—had been "physically presented for payment" at two locations in Ecuador, though no charges were actually incurred. To show standing, Whalen pointed to the two attempts to use her cards in Ecuador, the "risk of future identity fraud," and the lost time and money she spent resolving the attempted fraudulent purchases. But the Second Circuit held that Whalen failed to allege a concrete injury because (1) Whalen never paid, nor was asked to pay, for the attempted fraudulent charges in Ecuador; (2) she did not identify a threat of future fraud, as her stolen credit card had already been canceled and no other identifying information was stolen; and (3) the complaint did not allege that she expended any time or money to monitor her financial data.

Similarly, in *Reilly v. Ceridian Corp.* (3d Cir. 2011)—a pre-*Clapper* decision—a class of law firm employees brought a putative class action against a payroll processing firm (Ceridian) asserting various claims related to an increased risk of identity theft and costs to monitor credit activity after Ceridian suffered a security breach. Although the plaintiffs argued that the breach left them at an "increased risk of identity theft," they did not allege any actual misuse of personal information. The Third Circuit . . . found that the plaintiffs' alleged injuries were hypothetical and relied on speculation, and thus they were not "imminent" or "certainly impending." As a result, the plaintiffs did not have standing.

The Fourth Circuit has likewise rejected the "increased risk of future identity theft" theory in the context of a data breach. In *Beck v. McDonald* (4th Cir. 2017), a class of veterans who received medical treatment and health care at a South Carolina Veterans Affairs Medical Center brought actions alleging violations of various federal statutes following two data breaches at the Medical Center. The Fourth Circuit, distinguishing *Remijas* and *Krottner* on

---

[3] It is worth noting that the First Circuit appears to have gone both ways on this issue. In *Anderson v. Hannaford Bros.* (1st Cir. 2011), the First Circuit declined to question whether victims of a data breach—who alleged 1,800 instances of credit-card fraud—had standing to sue. But when analyzing *Anderson* in a different data breach case, the First Circuit drew the distinction between instances where confidential data has *actually* been accessed and case where data *might* be accessed. *Katz v. Pershing, LLC* (1st Cir. 2012). The Court held that, in the latter scenario, the "theoretical possibility" of access to confidential data "simply does not rise to the level of a reasonably impending threat." Since *Katz*, other Circuits have interpreted First Circuit law to preclude standing based on allegations of future identity theft unaccompanied by criminal activity involving the stolen information, as have district courts within the First Circuit.

the ground that those cases included allegations of actual misuse, found that the plaintiffs' alleged injury from the elevated risk of identity theft was "too speculative": "[E]ven after extensive discovery, the *Beck* plaintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information." The "mere theft" of the plaintiffs' data, without something more, required the consideration of the "attenuated chain of possibilities" rejected by *Clapper*. This theory of harm was simply "too speculative to constitute an injury-in-fact."[4]

And notably, the Eighth Circuit in *In re SuperValu, Inc.* (8th Cir. 2017) found no standing on an "increased risk of future identity theft" theory, even when a named plaintiff alleged actual misuse of personal information. There, a class of grocery store customers filed suit against SuperValu and other grocery store owner-operators following two data breaches in which the customers' financial information was allegedly accessed and stolen. The customers alleged that, as a result of the data breaches, hackers were allowed to gain access to customers' "names, credit or debit card account numbers, expiration dates, card verification value (CVV) codes, and personal identification numbers (PINs)." In support of their theory of standing, the customers relied on a June 2007 United States Government Accountability Office (GAO) report on data breaches, which states that "identity theft" includes "many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." That report points out, however, that compromised credit or debit card information, without additional personal identifying information, "generally cannot be used alone to open unauthorized new accounts." The Eighth Circuit additionally noted that the GAO report concludes that "most breaches have not resulted in detected incidents of identity theft."

In light of the GAO Report's findings, the Eighth Circuit found that the plaintiffs failed to demonstrate a substantial risk that they would suffer identity theft in the future. The hackers in *SuperValu* were not alleged to have stolen social security numbers, birth dates, or driver's license numbers, and thus, according to the GAO report, the risk of identity theft was "little to no[ne]." The Court did find, however, that a lone named plaintiff alleged actual misuse, and thus that plaintiff had standing based on *present*, but not *future* injury.

We are persuaded by the reasoning of the Eighth Circuit in *SuperValu*, and the facts of that case map closely to the facts of this one. Here, as the plaintiffs did in *SuperValu*, Tsao has alleged that hackers *may* have accessed and stolen customer credit card data "including the cardholder name, the account number, expiration date, card verification value ('CVV'), and PIN data for debit cards." Tsao has not alleged that social security numbers, birth dates, or driver's license numbers were compromised in the PDQ breach, and the card information allegedly accessed by the PDQ hackers "generally cannot be used alone to open unauthorized new accounts." So, based on the GAO Report, it is unlikely that the information allegedly stolen in the PDQ breach, standing alone, raises a substantial risk of identity theft.

This leaves us with the risk that the hackers, if they accessed and stole Tsao's credit card information, could make unauthorized purchases with his cards or drain his accounts. But again, the GAO Report suggests that most data breaches have not resulted in detected incidents of fraud on existing accounts. Indeed, the GAO Report reviewed the 24 largest data breaches between January 2000 and June 2005 and found that only 4 of the 24 breaches (roughly 16.667%) resulted in some form of identity theft, and only 3 resulted in account theft or fraud

---

[4] The Fourth Circuit later found standing in a data breach case where the plaintiffs did allege that hackers "used—and attempted to use—the Plaintiffs' personal information to open Chase Amazon Visa credit card accounts without their knowledge or approval." *Hutton v. Nat'l Bd. of Exam'rs in Optometry* (4th Cir. 2018).

(12.5%). Given the low rate of account theft, the GAO Report simply does not support the conclusion that the breach here presented a "substantial risk" that Tsao would suffer unauthorized charges on his cards or account draining.

Of course, we recognize that the GAO Report is over a decade old, and it is possible that some breaches may present a greater risk of identity theft than others. But even if we set aside the GAO Report and the reasoning of *SuperValu*, we remain unconvinced that Tsao has met his burden to show that the there is a "substantial risk" of harm, or that such harm is "certainly impending." Three considerations color this conclusion.

First, we recently held in *Muransky v. Godiva Chocolatier, Inc.* (11th Cir. 2020) that conclusory allegations of an "elevated risk of identity theft"—or, as Tsao puts it, a "continuing increased risk" of identity theft—"[are] simply not enough" to confer standing. Tsao's allegations about the "increased risk" of identity theft are supported only by reports defining identity theft, outlining the general risks of identity theft, or stating that identity thieves have stolen $112 billion in the last six years. These reports do nothing to clarify the risks to the plaintiffs *in this case*, and Tsao's threadbare allegations of "increased risk" are insufficient to confer standing.

Second, Tsao offers only vague, conclusory allegations that members of the class have suffered any actual misuse of their personal data—here, "unauthorized charges." But again, conclusory allegations of injury are not enough to confer standing. Of course, as our sister Circuits have recognized, evidence of actual misuse is not necessary for a plaintiff to establish standing following a data breach. *See, e.g., Beck* (stating that district court did not impermissibly require plaintiffs to demonstrate actual misuse). However, without specific evidence of *some* misuse of class members' data, a named plaintiff's burden to plausibly plead factual allegations sufficient to show that the threatened harm of future identity theft was "certainly impending"—or that there was a "substantial risk" of such harm—will be difficult to meet. As the case law discussed above confirms, most plaintiffs that have failed to offer at least some evidence of actual misuse of class members' data have fared poorly in disputes over standing.

Third, Tsao immediately cancelled his credit cards following disclosure of the PDQ breach, effectively eliminating the risk of credit card fraud in the future. Of course, even if Tsao's cards are cancelled, some risk of future harm involving identity theft (for example, the use of Tsao's name) still exists, but that risk is not substantial and is, at best, speculative.

We turn now to Tsao's claims that he has suffered actual, present injuries in his efforts to mitigate the risk of identity theft caused by the data breach.

Following notice of the PDQ data breach, Tsao notified Wells Fargo and Chase to cancel his credit cards and, in his words, "proactively t[ook] steps to mitigate the damage done by PDQ's mistakes." As a result of these mitigation efforts, Tsao claims that he has suffered three distinct injuries (1) lost opportunity to accrue cash back or rewards points on his cancelled credit cards, (2) costs associated with detection and prevention of identity theft in taking the time and effort to cancel and replace his credit cards; and (3) restricted account access to his preferred payment cards. Tsao's mitigation efforts are not enough to confer standing.

It is well established that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." In *Muransky*, this Court held that a plaintiff's mitigation costs—there, "additional time destroying or safeguarding his receipt"—were insufficient to confer standing because there was no substantial risk of identity theft. Although we noted that allegations of "wasted time" could sometimes "state a concrete harm for standing purposes," we noted that Muransky's "management-of-risk claim [wa]s bound up with his arguments about actual risk." As a result, Muransky's "assertion of wasted time and effort necessarily r[ose] or f[ell] along with" the Court's determination of whether there was a substantial risk of harm.

So too here. The mitigation costs Tsao alleges are inextricably tied to his perception of the actual risk of identity theft following the PDQ data breach. Tsao, by his own admission, voluntarily cancelled his credit cards, and the three types of harm he has identified flowed from that cancellation. By cancelling his cards, he voluntarily forwent the opportunity to accrue cash back or rewards points on those cards. By cancelling his cards, he voluntarily restricted access to his preferred payment cards. And by cancelling his cards, he voluntarily spent time safeguarding his accounts. Tsao cannot conjure standing here by inflicting injuries on himself to avoid an insubstantial, non-imminent risk of identity theft. To hold otherwise would allow "an enterprising plaintiff . . . to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." The law does not permit such a result.

We hold that Tsao lacks Article III standing because he cannot demonstrate that there is a substantial risk of future identity theft—or that identity theft is certainly impending—and because he cannot manufacture standing by incurring costs in anticipation of non-imminent harm. Accordingly, we affirm the District Court's order dismissing the case without prejudice for lack of standing.

JORDAN, Circuit Judge, concurring in the judgment.

Given our recent decision in *Muransky v. Godiva Chocolatier* (11th Cir. 2020) (en banc)—a decision from which I dissented—I concur in the judgment. I note only that the court here, rather than viewing Mr. Tsao's allegations favorably, necessarily engages in a value-laden and normative inquiry concerning the question of "substantial risk" at the motion-to-dismiss stage. That to me is problematic for a number of reasons, but *Muransky* apparently has sanctioned such an analytical approach. Hopefully the Supreme Court will soon grant certiorari in a case presenting the question of Article III standing in a data breach case.

Notes

1. How much does standing matter? On one hand, standing is crucial. Without standing, a federal court cannot exercise jurisdiction. Even if the parties do not raise the issue, federal courts have an independent obligation to ensure that they have jurisdiction over a case. But state courts are much more relaxed about standing than federal courts, and a dismissal from federal court for lack of standing does not bar a case from being brought in state court. In some areas of litigation, *plaintiffs* will argue that there is no standing because, without standing, a case cannot be removed into federal court.[224] So though lack of standing may stop a case in one court, the same claims and parties may proceed elsewhere.
2. *Tsao* is typical of standing cases. Federal courts are often reluctant to grant standing in data breach cases unless at least someone has suffered identity theft or some kind of tangible or traditional harm. In a classic breach of financial information or account numbers, freestanding claims of emotional harm and anxiety will generally not be credited. Fear of future impending harm will only be credited if it is justified by the presence of some harm that has already occurred. Similarly, the cost of precautions to mitigate the risk of future harm will only be credited if it is justified by some present harm. Once harm has occurred to at least some members of the class, however, all these other kinds of harm look substantially more imminent to courts.

Rather than hold that risk of future harm either is or is not sufficient, many circuits appear to have adopted a context sensitive approach. For example, the Fourth Circuit in *Beck v. McDonald*, 848 F.3d 262, 267 (4th Cir. 2017) declined to find standing "from the increased

[224] Whether being in state court favors plaintiffs or defendants is too complex a question to give a single universal answer. In general, however, many litigators (on both sides) are of the opinion that federal courts are better and more pleasant places to work, staffed with more qualified judges and law clerks, and supported by better-funded staff. What that has to do with Article III of the Constitution is unclear.

risk of future identity theft and the cost of measures to protect against it." Yet this conclusion was not unqualified. In the latter case *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 621–23 (4th Cir. 2018), the court distinguished *Beck*:

> In *Beck*, the plaintiffs alleged only a threat of future injury in the data breach context where a laptop and boxes—containing personal information concerning patients, including partial social security numbers, names, dates of birth, and physical descriptions—had been stolen, but the information contained therein had not been misused. The Plaintiffs in these cases, on the other hand, allege that they have already suffered actual harm in the form of identity theft and credit card fraud.
>
> At a minimum, Plaintiffs have sufficiently alleged an imminent threat of injury to satisfy Article III standing. On that score, these cases stand in stark contrast to *Beck*, where we concluded that the threat was speculative because "even after extensive discovery" there was "no evidence that the information contained on [a] stolen laptop [had] been accessed or misused or that [the plaintiffs had] suffered identity theft. In fact, there was no evidence that the thief even stole the laptop with the intent to steal private information. Here, the Plaintiffs allege that their data has been stolen, accessed, and used in a fraudulent manner.
>
> And although incurring costs for mitigating measures to safeguard against future identity theft may not constitute an injury-in-fact when that injury is speculative, the Court has recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists. The Complaints both allege that the Plaintiffs incurred out-of-pocket costs. And the Plaintiffs also suffered time lost in seeking to respond to fallout from the data breach. Indeed, they had to purchase credit monitoring services, and they had to notify credit reporting agencies and the IRS of the data breach of their personal information. Because the injuries alleged by the Plaintiffs are not speculative, the costs of mitigating measures to safeguard against future identity theft support the other allegations and together readily show sufficient injury-in-fact to satisfy the first element of the standing to sue analysis.

Given that some plaintiffs had suffered actual or attempted fraud, it was possible to find standing for not just them but also for plaintiffs who had not experienced fraud. Since that settlement size is ultimately related to number of plaintiffs, it matters a great deal whether the few who have had credit cards solicited in their names can create standing for the many who have not.

Consider the differences in the two cases:

In *Beck*, there was no evidence that the thief stole the laptop with the intent to access the personal information contained within. In *Hutton*, the National Board of Examiners in Optometry was intentionally hacked by cybercriminals.

In *Beck*, there was no evidence that the laptop thief accessed or even attempted to access the personal information held within. In *Hutton*, personal information of some plaintiffs was actually misused to open fraudulent bank accounts.

In *Beck*, there was no credit card information stored in the laptop, and although social security numbers are generally highly sensitive information, only parts of those numbers were stored. The fact that one particular plaintiff had unauthorized credit card charges did not elevate the sensitivity of the stolen information because credit card information could not have been obtained through the stolen laptop. In *Hutton*, plaintiffs' full social security numbers, names, dates of birth, addresses, and credit card information were stored in the breached database. The fact that hackers were able to open bank accounts, a process that requires

accurate personal information, corroborated the claim that highly sensitive information had been acquired.

When considering whether a breach poses a non-speculative risk of injury, it is helpful to consider three-factors:

1. whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data;
2. whether any portion of the dataset has already been misused, even if only a subset of the plaintiffs themselves have yet experienced identity theft or fraud; and
3. whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

Targeting is the sophisticated, intentional, and malicious acquisition of personal information, as opposed to the mere consequence of stealing a device with personal information stored within. Note that even if there was no evidence of targeting, the eventual misuse of personal information may show that the acquirer had intentions to do so.

Misuse of some plaintiffs' personal information creates a substantial risk of injury for all other plaintiffs, even those who have yet to experience actual or attempted misuse. This highlights the gravity of the situation and the need for comprehensive measures to address and prevent such risks.

Sensitivity of exposed information is a fact-intensive inquiry, as it relates to how useful the information could be in committing identity theft. As noted before the *Tsao* excerpt and in the case itself, plaintiffs are not liable for fraudulent credit card charges and credit cards may be reissued with ease, rendering mitigation expenses for credit monitoring extreme measures for an unlikely harm. On the other hand, an exposed social security number, along with name, date of birth, and address, is precisely the set of information needed to open a bank account, and its utility in other transactions creates a need for constant monitoring of future misuse.

In addition to standing, courts also must consider the substance of data breach claims. Consider the below case looking at one of the largest domestic data breaches. Note the multiplicity of claims and jurisdictions.

In re Equifax, Inc., Customer Data Security Breach Litig., 362 F.Supp.3d 1295 (N.D. Ga. 2019)

THOMAS W. THRASH, JR., United States District Judge

On September 7, 2017, the Defendant Equifax Inc. announced that it was the subject of one of the largest data breaches in history. From mid-May through the end of July 2017, hackers stole the personal and financial information of nearly 150 million Americans. During this time period, Equifax failed to detect the hackers' presence in its systems, allowing the hackers to exfiltrate massive amounts of sensitive personal data that was in the company's custody. This data breach ("Data Breach") is unprecedented—it affected almost half of the entire American population. The Data Breach was also severe in terms of the type of information that the hackers were able to obtain. The hackers stole at least 146.6 million names, 146.6 million dates of birth, 145.5 million Social Security numbers, 99 million addresses, 17.6 million driver's license numbers, 209,000 credit card numbers, and 97,500 tax identification numbers. This is extremely sensitive personal information. Using this information, identity thieves can create fake identities, fraudulently obtain loans and tax refunds, and destroy a consumer's creditworthiness.

Equifax Inc. is a Georgia corporation with its principal place of business in Atlanta, Georgia. Equifax is the parent company of the Defendants Equifax Information Services LLC and Equifax Consumer Services LLC. The Defendants operate together as an integrated

consumer reporting agency. The Plaintiffs are 96 consumers who allege that they have been injured by the Data Breach. They allege that they are suffering a "present, immediate, imminent, and continuing increased risk of harm" due to the compromise of their personally identifiable information in the Data Breach. The Plaintiffs seek to represent a class of those similarly situated consumers in the United States who were injured by the Data Breach.

Equifax's business model entails aggregating data relating to consumers from various sources, compiling that data into credit reports, and selling those reports to lenders, financial companies, employers, and others. Credit reporting agencies are "linchpins" of the nation's financial system due to the importance of credit reports in decisions to extend credit. Equifax also sells this information directly to consumers, allowing consumers to purchase their credit files and credit scores. In recent years, Equifax has worked to rapidly grow its business. Recognizing the value in obtaining massive troves of consumer data, Equifax has aggressively acquired companies with the goal of expanding into new markets and acquiring new sources of data. Equifax now maintains information on over 820 million individuals and 91 million businesses worldwide.

Equifax recognized the importance of data security, and the value of the data in its custody to cybercriminals. Equifax observed other major, well-publicized data breaches, including those at Target, Home Depot, Anthem, and its competitor Experian. Equifax held itself out as a leader in confronting such threats, offering "data breach solutions" to businesses. It also acquired two identity theft protection companies, Trusted ID and ID Watchdog. Equifax was also the subject of several prior data breaches. From 2010 on, Equifax suffered several different data breach incidents highlighting deficiencies in its cybersecurity protocol. Given these prior breaches, cybersecurity experts concluded that Equifax was susceptible to a major data breach. Analyses of Equifax's cybersecurity demonstrated that it lacked basic maintenance techniques that are highly relevant to potential data breaches. However, despite these risks, Equifax did little to improve its cybersecurity practices. Equifax's leaders afforded low priority to cybersecurity, spending a small fraction of the company's budget on cybersecurity.

The story of the Data Breach begins on March 6, 2017. On that date, a serious vulnerability in the Apache Struts software was discovered and reported. This software, a popular open-source program, was used by Equifax in its consumer dispute portal website. The next day, the Apache Software Foundation issued a free patch and urged all users to immediately implement the patch. The Department of Homeland Security also issued warnings concerning this vulnerability. Equifax internally disseminated the warning, but never implemented the patch. Then, beginning on May 13, 2017, hackers were able to manipulate the Apache Struts vulnerability to access Equifax's systems, and using simple commands determined the credentials of network accounts that allowed them to access the confidential information of millions of American consumers. From May 13 to July 30, 2017, the hackers remained undetected in Equifax's systems. During this time, the hackers were able to steal the sensitive personally identifiable information of approximately 147.9 million American consumers. The personally identifiable information that hackers obtained in the Data Breach includes names, addresses, birth dates, Social Security numbers, driver's license information, telephone numbers, email addresses, tax identification numbers, credit card numbers, credit report dispute documents, and more.

On July 29, 2017, Equifax's security team noticed "suspicious network traffic" in the dispute portal. The next day, the consumer dispute portal was deactivated and taken offline. On July 31, 2017, Equifax's CEO Richard Smith was informed of the breach. On August 2, 2017, Equifax informed the Federal Bureau of Investigation about the Data Breach, and retained legal counsel to guide its investigation. Equifax also hired cybersecurity firm Mandiant to investigate the suspicious activity. On September 7, 2017, seven weeks after discovering suspicious activity, Equifax publicly disclosed the Data Breach in a press release. Experts have

since opined that the Data Breach was the result of weak cybersecurity measures and Equifax's low priority for data security.

The Plaintiffs here are a putative class of consumers whose personal information was stolen during the Data Breach. The class alleges that it has been harmed by having to take measures to combat the risk of identity theft, by identity theft that has already occurred to some members of the class, by expending time and effort to monitor their credit and identity, and that they all face a serious and imminent risk of fraud and identity theft due to the Data Breach. The putative class brings a number of nationwide claims, along with a number of state claims. The class also seeks declaratory and injunctive relief. The Defendants now move to dismiss.

Legally Cognizable Injury

The Defendants next argue that all of the Plaintiffs' tort claims, including their negligence, negligence per se, and state consumer protection act violations, fail because they have not sufficiently alleged injury and proximate causation. According to the Defendants, the Plaintiffs' injuries are not legally cognizable harms, and even if they were, the Plaintiffs have failed to adequately allege that the Defendants proximately caused their harms. Finally, the Defendants argue that the Plaintiffs' tort claims are all barred by the economic loss doctrine.

1. Non-Harms and Speculative Future Harms

First, the Defendants contend that the Plaintiffs have not pleaded legally cognizable harms because their purported injuries only include "non-harms" and "speculative future harms." "It is well-established Georgia law that before an action for a tort will lie, the plaintiff must show he sustained injury or damage as a result of the negligent act or omission to act in some duty owed to him." "Although nominal damages can be awarded where there has been an injury but the injury is small, . . . where there is no evidence of injury accompanying the tort, an essential element of the tort is lacking, thereby entitling the defendant to judgment in his favor."

The Defendants first contend that the compromise of personally identifiable information itself is not an injury. Each of the Plaintiffs alleges that his or her personally identifiable information was compromised in the Data Breach. Such an injury is legally cognizable under Georgia law. The cases relied upon by the Defendants are distinguishable. The Defendants cite *Rite Aid of Georgia, Inc. v. Peacock* (Ga. Ct. App. 2012) for the proposition that a plaintiff suffers no injury from the illegal sale of personally identifiable information. However, as the Plaintiffs point out, the plaintiff in that case did not allege that this information was misused, or likely to be misused. In *Rite Aid*, the plaintiff's pharmacy records were sold from Rite Aid to Walgreens when a Rite Aid store was closing. The plaintiff sought certification of a class of all individuals whose information had been sold to Walgreens. The court concluded that class certification was not proper, in part, because the plaintiff had not alleged an injury from the sale of his information from one pharmacy to the other, and instead only alleged a violation of law. In contrast, the Plaintiffs here have alleged that they have been harmed by having to take measures to combat the risk of identity theft, by identity theft that has already occurred to some members of the class, by expending time and effort to monitor their credit and identity, and that they all face a serious and imminent risk of fraud and identity theft due to the Data Breach. These allegations of actual injury are sufficient to support a claim for relief.

The Defendants also cite *Finnerty v. State Bank & Trust Company* (Ga. Ct. App. 2009) for the proposition that fear of future damages from identity theft is too speculative to form a basis of recovery. However, as the Plaintiffs emphasize, that case involved an invasion of privacy claim by an individual whose Social Security number was included in a public court filing. The court concluded that this claim failed because, to state a claim for invasion of privacy, a plaintiff must show that there was a public disclosure in which information is distributed to the public at large. There, the claimant failed to allege that anyone actually saw his Social

Security number, and thus did not prove that there was a public disclosure. Thus, the court there did not hold that the disclosure of personal information is, as a matter of law, not a legally cognizable injury. Instead, it concluded that one of the elements of an invasion of privacy claim was not met, making it distinguishable from this case. And, in contrast to the inadvertent disclosure of a Social Security number in a single public court filing, the compromise of a huge amount of personally identifying information by criminal hackers presents a much more significant risk of identity fraud.

The Defendants also cite *Randolph v. ING Life Insurance and Annuity Company* (D.C. Ct. App. 2009). There, the plaintiffs sued after a laptop computer containing their personal information was stolen from the home of one of the defendant's employees, alleging that there was a substantial risk of identity theft and other dangers due to the possible unauthorized use of their personal information. In that case, there was no evidence that the theft occurred for the specific purpose of obtaining the information on the laptop as opposed to the computer itself. Here, by contrast, the Plaintiffs allege that their information was specifically targeted and has already been misused. The Plaintiffs have adequately alleged facts showing actual cognizable injury.

2. Proximate Causation

The Defendants next contend that the Plaintiffs have failed to adequately allege that Equifax proximately caused their injuries. "[B]efore any negligence, even if proven, can be actionable, that negligence must be the proximate cause of the injuries sued upon." "To establish proximate cause, a plaintiff must show a legally attributable causal connection between the defendant's conduct and the alleged injury." A plaintiff must establish "that it is more likely than not that the conduct of the defendant was a cause in fact of the result." "A mere possibility of such causation is not enough; and when the matter remains one of pure speculation or conjecture, or the probabilities are at best evenly balanced, it becomes the duty of the court to grant summary judgment for the defendant."

First, the Defendants argue that the Plaintiffs fail to allege that any injuries resulting from identity theft, payment-card fraud, or other similar theories resulted specifically from the Equifax Data Breach, and not some other data breach or fraudulent conduct. According to the Defendants, the Plaintiffs highlight dozens of other security breaches dating to 2013 in the Complaint, and the Defendants assert that over 1,500 data breaches occurred in 2017 alone. Thus, since the Plaintiffs have failed to allege that their injuries resulted directly from their personal information being obtained in this specific Data Breach, their theory of causation is "guesswork at best."

However, the Court finds this argument unpersuasive. Many of the Plaintiffs have alleged in the Complaint that they suffered some form of identity theft or other fraudulent activity as a result of the Data Breach. Such an allegation is sufficient at the pleading stage to establish that the Data Breach was the proximate cause of this harm. The Plaintiffs need not explicitly state that other breaches did *not* cause these alleged injuries, since their allegations that this Data Breach *did* cause their injuries implies such an allegation. Furthermore, allowing the Defendants "to rely on other data breaches to defeat a causal connection would 'create a perverse incentive for companies: so long as enough data breaches take place, individual companies will never be found liable.'" The Court declines to create such a perverse incentive.

Many of the Plaintiffs also allege in the Complaint that they purchased credit monitoring and incurred other costs in direct response to the Data Breach. Thus, even assuming their identity theft injuries resulted from previous breaches, these separate injuries resulted only from the occurrence of the Data Breach. Finally, even assuming that such an argument could disprove proximate causation, it presents a factual dispute most appropriate for a jury to consider. The Plaintiffs have alleged that the Data Breach caused their identities to be stolen,

while the Defendants contend prior breaches caused these injuries. This is purely a dispute of fact that is not appropriate for resolution at this stage of the litigation. Therefore, the Court concludes that the Plaintiffs have adequately alleged that the Data Breach proximately caused their injuries. The Plaintiffs plausibly allege that Equifax had custody of their personally identifiable information, that Equifax's systems were hacked, that these hackers obtained this personal information, and that as a result of this breach, they have become the victims of identity theft and other fraudulent activity. This is sufficient.

Next, the Defendants contend that the Plaintiffs' injuries were proximately caused by an "unidentified third party's criminal acts," and not Equifax itself. According to the Defendants, the unforeseeable criminal acts of third parties "insulate" defendants from liability. "Generally, there is no duty to prevent the unforeseeable 'intervening criminal act of a third person.'" Under Georgia law, "when a defendant claims that its negligence is not the proximate cause of the plaintiff's injuries, but that an act of a third party intervened to cause those injuries, the rule is 'that an intervening and independent wrongful act of a third person producing the injury, and without which it would not have occurred, should be treated as the proximate cause, insulating and excluding the negligence of the defendant.'"

However, "this rule does not insulate the defendant 'if the defendant had reasonable grounds for apprehending that such wrongful act would be committed.'" "[I]f the character of the intervening act claimed to break the connection between the original wrongful act and the subsequent injury was such that its probable or natural consequences could reasonably have been anticipated, apprehended, or foreseen by the original wrongdoer, the causal connection is not broken, and the original wrongdoer is responsible for all of the consequences resulting from the intervening act." Thus, if the Defendants had reasonable grounds to anticipate the criminal act, then they are not insulated from liability. "In determining whether a third-party criminal act is foreseeable, Georgia courts have held that 'the incident causing the injury must be substantially similar in type to the previous criminal activities . . . so that a reasonable person would take ordinary precautions to protect his or her customers or tenants against the risk posed by that type of activity.'" The question of reasonable foreseeability of a criminal attack is generally for a jury to determine. However, it may not be in this case because of the many public statements by Equifax that it knew how valuable its information was to cyber criminals and its susceptibility to hacking attempts.

The Court concludes that, as in *In re Arby's Restaurant Group Inc. Litigation* (N.D. Ga. 2018) and *In re: The Home Depot, Inc., Customer Data Security Breach Litigation* (N.D. Ga. 2016), the criminal acts of the hackers were reasonably foreseeable to the Defendants, and thus do not insulate them from liability. In the Complaint, the Plaintiffs allege that the Defendants observed major data breaches at other corporations, such as Target, Anthem, and Experian. Equifax itself even experienced prior data breaches. Furthermore, Equifax ignored warnings from cybersecurity experts that its data systems were dangerously deficient, and that there was a substantial risk of an imminent breach. These allegations are sufficient to establish that the acts of the third party cyberhackers were reasonably foreseeable. Thus, the causal chain is not broken.

Negligence

Next, the Defendants move to dismiss the Plaintiffs' negligence claim. In Count 2 of the Complaint, the Plaintiffs allege that Equifax owed a duty to the Plaintiffs to "exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons." The Plaintiffs also allege that Equifax had a duty of care that arose from Section 5 of the Federal Trade Commission Act (the "FTC Act"), and the FCRA. The Defendants contend that they were under no duty of care toward the Plaintiffs.

In Georgia, "[a] cause of action for negligence requires (1) [a] legal duty to conform to a standard of conduct raised by the law for the protection of others against unreasonable risks of harm; (2) a breach of this standard; (3) a legally attributable causal connection between the conduct and the resulting injury; and, (4) some loss or damage flowing to the plaintiff's legally protected interest as a result of the alleged breach of the legal duty." "The threshold issue in any cause of action for negligence is whether, and to what extent, the defendant owes the plaintiff a duty of care." Whether such a duty exists is a question of law. Georgia recognizes a general duty "to all the world not to subject them to an unreasonable risk of harm."

The Defendants contend that Georgia law does not impose a duty of care to safeguard personal information. The Defendants rely primarily upon a recent Georgia Court of Appeals case, *McConnell v. Georgia Department of Labor* (Ga. Ct. App. 2018). In *McConnell*, the plaintiff filed a class action against the Georgia Department of Labor after one of its employees sent an email to 1,000 Georgians who had applied for unemployment benefits. This email included a spreadsheet with the name, Social Security number, phone number, email address, and age of 4,000 Georgians who had registered for services with the agency. The plaintiff, whose information was disclosed, filed a class action, asserting, among other claims, a claim for negligence.

The Court concludes that, under the facts alleged in the Complaint, Equifax owed the Plaintiffs a duty of care to safeguard the personal information in its custody. This duty of care arises from the allegations that the Defendants knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures. *McConnell III* [the most recent of the *McConnell* opinions] does not alter this conclusion. As the court in *McConnell I* [the earliest of the *McConnell* line] noted, a critical distinction between these cases is that the duty in *Home Depot* arose from allegations that the defendant failed to implement reasonable security measures in the face of a known security risk. Such allegations did not exist in the *McConnell* line of cases. The *McConnell III* court came to the same conclusion as the *McConnell I* court, and did nothing to dispel this distinction made in *McConnell III*. Furthermore, given this mention of *Home Depot* in *McConnell I*, and the court's subsequent holding in *Arby's*, the *McConnell III* court's silence on this issue suggests a tacit approval of this distinction. And, as this Court noted in *Home Depot*, to hold otherwise would create perverse incentives for businesses who profit off of the use of consumers' personal data to turn a blind eye and ignore known security risks.

The Defendants go to great lengths to distinguish the Georgia Supreme Court's decision in *Bradley Center, Inc. v. Wessner* (Ga. 1982). Both *Home Depot* and *Arby's* relied, in part, upon *Wessner* to conclude that the defendants were under a duty to take reasonable measures to avoid a foreseeable risk of harm from a data breach incident. In *Wessner*, a man who voluntarily committed himself to a psychiatric hospital made statements to the hospital's staff that he desired to harm his wife. Despite these statements, the man was issued a weekend pass by the staff, and he subsequently obtained a gun, confronted his wife and another man, and killed them both. The Georgia Supreme Court concluded that the hospital owed a duty of care to the man's wife. The court explained that "[t]he legal duty in this case arises out of the general duty one owes to all the world not to subject them to an unreasonable risk of harm."

The Defendants argue that the holding in *Wessner* is much narrower than this. According to them, *Wessner* merely stands for the narrow proposition that a physician owes a legal duty when, in the course of treating a mental health patient, that physician exercises control over the patient and knows or should know that the patient is likely to cause harm to others. The Defendants further assert that the *Wessner* court's references to general negligence principles were done in an effort to explain why the case was a negligence case, and not a medical malpractice case. However, despite the Defendants' efforts to minimize the importance of *Wessner*, the Court finds that *Wessner* supports the conclusion that the Defendants owed a legal duty to take reasonable measures to prevent a reasonably foreseeable risk of harm due to

a data breach incident. Nowhere in the *Wessner* decision does the Georgia Supreme Court limit its holding to the narrow proposition that the Defendants assert. In fact, in *Wessner*, the court explained that it was not creating a "new tort," but instead that it was applying "our traditional tort principles of negligence to the facts of this case." Other Georgia cases have similarly applied these same general principles. Likewise, this Court concludes that, under traditional negligence principles, the Defendants owed a legal duty to the Plaintiffs to take reasonable precautions due to the reasonably foreseeable risk of danger of a data breach incident.

Georgia Fair Business Practices Act

Next, the Defendants move to dismiss the Plaintiffs' claims under the Georgia Fair Business Practices Act. The Georgia Fair Business Practices Act prohibits, generally, "unfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce."

The Defendants first argue that the Georgia Fair Business Practices Act does not require the safeguarding of personally identifiable information. According to the Defendants, *McConnell III* would have been decided differently if the Georgia Fair Business Practices Act contained such a requirement. In *McConnell III*, the court concluded that part of the Georgia Fair Business Practices Act, O.C.G.A. § 10-1-393.8, "cannot serve as the source of such a general duty to safeguard and protect the personal information of another." That provision prohibited "intentionally communicating a person's social security number." The court rejected the plaintiff's claim, noting that he had alleged that the defendant negligently disseminated his social security number.

The Plaintiffs make multiple arguments in response. However, the Court finds these arguments unpersuasive. First, they argue that *Arby's II*, decided after *McConnell III*, held that data breach victims can pursue a claim under the Georgia Fair Business Practices Act. However, that decision only considered whether the plaintiffs had adequately alleged reliance. Thus, the court's reasoning does not bear on whether *McConnell III* precluded recovery under the Georgia Fair Business Practices Act. Second, the Plaintiffs contend that *McConnell III* only stands for the proposition that the Georgia Fair Business Practices Act is not the basis of a general tort duty. However, *McConnell III's* holding was broader than that. In *McConnell III*, the court, after examining parts of the Georgia Fair Business Practices Act, along with the Georgia Personal Identity Protection Act, concluded that there is no statutory basis for a duty to safeguard personal information in Georgia. It further explained that the Georgia legislature has not acted to establish a standard of conduct to protect the security of personal information, unlike other jurisdictions with data protection and data breach laws. Even though *McConnell III* examined the Georgia Fair Business Practices Act in the context of its provisions dealing with Social Security numbers specifically, it concluded that the entire Act, along with the rest of Georgia statutory law, did not require the safeguarding of personal information. Therefore, the Court concludes that the Georgia Fair Business Practices Act does not require businesses to safeguard personally identifiable information. This issue may be revisited depending upon the ruling of the Georgia Supreme Court in *McConnell III*.

State Statutes

[1. State Business Fraud and Consumer Protection Statutes discussion omitted]

2. State Data Breach Notification Statutes

Next, the Defendants move to dismiss the Plaintiffs' claims under state data breach notification statutes. The Defendants contend that twelve of the data breach statutes under which the Plaintiffs assert claims do not allow private rights of action. According to the Defendants, the data breach statutes of Colorado, Delaware, Florida, Iowa, Kansas, Maryland, Michigan, Montana, New Jersey, New York, Wisconsin, and Wyoming do not permit private actions, and the Georgia statute is silent as to whether a private right of action exists.

The Plaintiffs contend that, with regard to the statutes of Iowa, Michigan, and New York, this argument ignores the statutory language. According to the Plaintiffs, courts have interpreted these statutes to be ambiguous as to this question, or that they provide non-exclusive remedies. Iowa's data-breach statute provides that "[a] violation of this chapter is an unlawful practice pursuant to section 714.16 and, in addition to the remedies provided to the attorney general pursuant to section 714.16, subsection 7, the attorney general may seek and obtain an order that a party held to violate this section pay damages to the attorney general on behalf of a person injured by the violation." However, it further provides that "[t]he rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law." In *Target*, the court concluded that "[t]his is at least ambiguous as to whether private enforcement is permissible," and thus the Iowa claims should not be dismissed. The Defendants contend that this Court should not follow *Target* where its reasoning is "plainly and persuasively contradicted by other courts or the statutes themselves." However, the Defendants have provided no cases contradicting this reasoning, and the *Target* holding is not inconsistent with the language of the statute. Therefore, this Court likewise concludes that the Plaintiffs' claims under the Iowa data-breach statute should not be dismissed for this reason. [Similar argument regarding Michigan's data-breach statute omitted]

Next, New York's statute provides that "whenever the attorney general shall believe from evidence satisfactory to him that there is a violation of this article he may bring an action in the name and on behalf of the people of the state of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation." The statute also provides that "the remedies provided by this section shall be in addition to any other lawful remedy available." At first glance, these claims should survive for the same reasons the Iowa and Michigan claims survived in *Target*. However, this statute also provides that "[t]he provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section." A New York state court interpreted this provision to preclude a private action, reasoning that the "language . . . militates against any implied private right of action" because it would be inconsistent with the legislative scheme. The Court agrees with this reasoning. Thus, since no private right of action exists under New York's data-breach statute, the Plaintiffs' claims under section 899-aa should be dismissed.

The Plaintiffs then contend that four of the data-breach statutes, those of Connecticut, Maryland, Montana, and New Jersey, are enforceable through those states' consumer-protection statutes, even though the data-breach statutes themselves do not contain a private right of action. The Plaintiffs contend that violation of Connecticut's data-breach statute constitutes an unfair trade practice enforceable through its unfair trade practices statute. However, section 36a-701b explicitly states that "[f]ailure to comply with the requirements of this section shall constitute an unfair trade practices for purposes of section 42-110b *and shall be enforced by the Attorney General*." The Plaintiffs, in their brief, conspicuously omit the last part of this provision, which explicitly limits enforcement to the Attorney General. Thus, the Plaintiffs' claims under section 36a-701b should be dismissed. Similarly, the Maryland and Montana data breach statutes are also privately enforceable through those states' unfair trade practices statutes.

The Court similarly concludes that New Jersey's statute provides a private right of action. Furthermore, the data breach statutes of Colorado, Delaware, Kansas, and Wyoming contain ambiguous language as to private enforceability or provide that the statute's remedies are "non-exclusive." In *Target*, the court noted that this permissive language is "at least ambiguous as to whether there is a private right of action" and concluded that, "absent any authority construing this ambiguity to exclude private rights of action," the claims should not be dismissed. The Court finds this reasoning persuasive. The Defendants have not identified any authority construing this language as precluding private rights of action. Absent such

authority, the Court declines to dismiss the Plaintiffs' claims under the Colorado, Delaware, Kansas, and Wyoming data breach statutes.

Finally, Georgia's statute is silent as to whether a private right of action exists. Here, the Defendants cite Georgia authority to support the proposition that such silence suggests no private right of action exists. Therefore, the claims under O.C.G.A. § 10-1-912 should be dismissed.

Next, the Defendants argue that the Plaintiffs have failed to adequately allege a violation of any of the state data breach notification statutes. According to the Defendants, the Complaint alleges that 41 days elapsed between Equifax's discovery of the Data Breach and the disclosure of the incident to the public. The Defendants contend these state data-breach statutes permit an entity time to determine the scope of a breach before notification, and several of the statutes even establish specific time limits. Therefore, according to the Defendants, their notification met the requirements of these statutes.

However, the Court concludes that the Plaintiffs have adequately alleged a violation of many of these statutes. These statutes require notification, for example, in "the most expedient time possible and without unreasonable delay" and, for example, within a reasonable time. The Plaintiffs have alleged facts from which a jury could conclude that the Defendants did not provide notice within a reasonable time, as these notification statutes require. Therefore, the Court concludes that the Plaintiffs have adequately stated a claim.

Finally, the Defendants contend that the Plaintiffs have failed to allege any injury resulting from a delay in notification. According to the Defendants, the Plaintiffs have not alleged when any injury occurred, and thus have not alleged any damage occurring between the time that Equifax should have notified them of the Data Breach, and the time that Equifax did publicly disclose the Data Breach. However, the *Target* court rejected this exact argument. There, the court reasoned that such an argument is premature at this stage and that plaintiffs need only plead "a 'short and plain statement' of their claims" under Rule 8. The Plaintiffs note that they could have frozen their credit earlier, or taken other precautions. At this stage of the litigation, such allegations are sufficient.

Notes

1. Notice that this case has no discussion of standing. In a footnote, the court said "Importantly, the Defendants do not seem to contend that the Plaintiffs have failed to establish standing. Instead, the Defendants contend that the Plaintiffs have not established a legally cognizable harm, or proximate causation, as elements of a tort claim." Is it clear there is standing here?
   Sometimes defendants argue in favor of standing because it means that they can keep the case in federal court. If a major corporation is forced to litigate *somewhere*, it will often prefer to do so there. Also, once a case moves into "settlement approval" territory, incentives completely change. Suddenly all the major parties want the court to have jurisdiction and sign off on the proposed deal. Objectors will sometimes raise standing concerns, and they did so here. The 11th Circuit affirmed the district court's finding of standing, however. Specifically, it noted that the information stolen could be used to create fake identities, fraudulently obtain loans and tax returns, and destroy a consumer's credit worthiness. Further, the consumers faced heightened risk of future identity theft (proven by the identity theft suffered by others in the class) and had spent "time, money, or effort dealing with the breach."

   > Beyond the sufficient risk of identity theft and resulting injuries, a vast number of Plaintiffs who have not yet suffered identity theft also allege they have spent time, money, and effort mitigating the risk of identity theft. Their efforts include purchasing credit freezes, monitoring their financial accounts, and purchasing credit monitoring, among other things. As explained above, because the risk of

> harm here is a sufficient injury, the allegations of mitigation injuries made by these Plaintiffs are also sufficient. Plaintiffs have easily shown an injury in fact.

In re Equifax Inc. Customer Data Sec. Breach Litig., 999 F.3d 1247, 1263 (11th Cir. 2021)

2. This case hits on all the major issues that are raised in data breach cases. Is there a duty to keep the plaintiffs' data secure? If so, does that duty exist in every state, or should only a portion of the class proceed? Was the plaintiff class actually harmed? If so, how much? Is that harm fairly traceable to the defendant's conduct?
   Key to the negligence discussion was whether Equifax owed a fiduciary duty of care to the consumers and their personal information. Different jurisdictions have different law on this point, but often parallels are drawn from fiduciary relationships such as the one between a medical provider and a patient. Hospitals, for instance, owe a duty of care to patients and their information because patients are required to provide highly sensitive information to hospitals to receive medical care.
   Breach of implied contract is another claim that receives varying treatment across jurisdictions. It will often matter whether the data security claim in the privacy policies is express and detailed, but even a vague promise of data security may be read to require adherence to industry standards.
3. Key in these cases is defining the source of the legal violation. Different causes of action give rise to different plaintiff classes and different damages calculations. A claim that notification should have gone out a week earlier can be fairly said to have lower damages than a claim that the company should have had better data security and avoided the breach entirely. Plaintiffs here also sued for a violation of the Fair Credit Reporting Act, breach of contract (on behalf of those who had credit monitoring through Equifax), unjust enrichment, negligence per se (see the discussion after *LabMD*, below), and violation of state statutes on fair dealing. The goal is generally to assemble the largest possible class with the broadest possible theory of liability and damages to force the highest possible settlement.
4. After this case was decided, the Georgia Supreme Court issued *McConnell IV*, which dismissed the claim against the Georgia Department of Labor and repudiated some of the case law cited here ("Accordingly, we hereby disapprove *Bradley Center [v. Wessner]* to the extent that it created a general legal duty 'to all the world not to subject [others] to an unreasonable risk of harm.'"). Then the Georgia Supreme Court issued *Collins v. Athens Orthopedic Clinic, P.A.,* 307 Ga. 555, 561 (2019), which allowed a negligence claim for a medical data breach to go forward. The District Court in *Equifax* held that none of this activity changed its opinion on the duty of care given the heavily regulated nature of the credit reporting industry. *In re Equifax, Inc., Customer Data Sec. Breach Litig.,* No. 1:17-MD-2800-TWT, 2022 WL 1122841, at *8 (N.D. Ga. Apr. 13, 2022).
5. Equifax was also sued by the Federal Trade Commission and a coalition of 50 attorney generals (48 states, D.C., and Puerto Rico). It settled the suit for up to $425 million to affected consumers, $175 million to the states, and injunctive relief requiring it to upgrade its data security and assist identity theft victims. This action separately settled for $380.5 million for a Consumer Restitution Fund and attorney fees, with potential to increase by $125 million for certain out-of-pocket losses if that proved insufficient; free credit monitoring, which would have an estimated cost of $2 billion if all 147 million class members signed up; and a minimum of $1 billion for data security and related technology over five years. The Consumer Restitution Fund in this case supplanted the one that would have been established by the FTC settlement.

C. Federal Trade Commission and Data Security

As discussed in Chapter 9, the Federal Trade Commission (FTC) has extensive power under its Section 5 authority to regulate behaviors in commerce that are unfair or deceptive. The FTC also has power under a variety of statutes, such as the Fair Credit Reporting Act and

Gramm–Leach–Bliley, to regulate data security in some specific contexts. As such, the FTC has been active in the data security domain for decades.

The FTC has repeatedly published guidelines to advise companies on data security. Its 2015 publication "Start with Security" gives a basic overview. Consider its 10 points.[225]

1. Start with security. Collecting and maintaining information "just because" is no longer a sound business strategy. Instead, deliberately think through the implications of your data decisions. No one can steal what you don't have. When does your company ask people for sensitive information? Keep information only so long as you need it and don't collect it if you don't need it.
2. Control access to data sensibly. Not everyone on your staff needs unrestricted access to your network and the information stored on it. Put controls in place to make sure employees have access only on a "need-to-know" basis. For your network, consider steps such as separate user accounts to limit access to the places where personal data is stored or to control who can use particular databases. Restrict access to sensitive data and limit administrative access to control the scope of any breach.
3. Require secure passwords and authentication. In *In the Matter of Drizly, Inc.*, the FTC alleged the company failed to require unique and complex passwords or multifactor authentication for accessing the company's GitHub repositories. A Drizly executive reused a password he had used for other personal accounts, and his recycled password was exposed in an unrelated breach. This created an opportunity for a malicious actor to access Drizly's GitHub repositories, which made it possible for the attacker to access other database credentials and ultimately exfiltrate the personal information of 2.5 million consumers.
4. Store sensitive personal information securely and protect it during transmission. Even if you take appropriate steps to secure your network, sometimes you have to send that data elsewhere. Use strong cryptography to secure confidential material during storage and transmission. The method will depend on the types of information your business collects, how you collect it, and how you process it.
5. Segment your network and monitor who's trying to get in and out. When designing your network, consider using tools to validate and limit implicit trust between networked systems. Assume that all traffic regardless of source is hostile. Part of your "zero trust" toolkit should be tools to inspect and log network traffic to monitor your network for malicious activity.
6. Secure remote access to your network. Ensure that computers with remote access to their networks have appropriate endpoint security, and limit off-site employee and vendor access to the minimum necessary.
7. Apply sound security practices when developing new products. Really, just "start with security" as applied to new lines of business.
8. Make sure your service providers implement reasonable security measures. Don't assume that your various vendors and subcontractors have good data security. Impose paperwork requirements so they are on notice about security expectations *and* conduct audits.
9. Put procedures in place to keep your security current and address vulnerabilities that may arise. Expect that new vulnerabilities will be discovered and regularly patch and update your various systems.
10. Secure paper, physical media, and devices. Remember that it is possible to have a data breach from unshredded documents, unwiped surplus equipment, and misplaced laptops.

Most of these points are good advice. They are, however, very basic. This makes them somewhat timeless while simultaneously limiting their usefulness once a company gets through the very early stages of planning its data security approach. In addition to the points above, the

[225] Titles from their document, contents paraphrased by the author. For the full document, go to https://www.ftc.gov/business-guidance/resources/start-security-guide-business.

FTC has been particularly interested in promoting multifactor authentication in recent years. That interest has appeared in several recent consent decrees.

Though the FTC would like companies to follow these guidelines, it is unclear where the line is between "good idea" and "legal requirement." Companies need not "start with security" and many companies (outside of those few states with strong consumer privacy laws) continue to collect all information possible "just because." Yet the FTC can and does sue companies over data security problems.

FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015)

AMBRO, Circuit Judge.

The Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce." In 2005 the Federal Trade Commission began bringing administrative actions under this provision against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers. The vast majority of these cases have ended in settlement.

On three occasions in 2008 and 2009 hackers successfully accessed Wyndham Worldwide Corporation's computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges. The FTC filed suit in federal District Court, alleging that Wyndham's conduct was an unfair practice and that its privacy policy was deceptive. The District Court denied Wyndham's motion to dismiss, and we granted interlocutory appeal on two issues: whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision. We affirm the District Court.

Wyndham Worldwide is a hospitality company that franchises and manages hotels and sells timeshares through three subsidiaries. Wyndham licensed its brand name to approximately 90 independently owned hotels. Each Wyndham-branded hotel has a property management system that processes consumer information that includes names, home addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes. Wyndham "manage[s]" these systems and requires the hotels to "purchase and configure" them to its own specifications. It also operates a computer network in Phoenix, Arizona, that connects its data center with the property management systems of each of the Wyndham-branded hotels.

The FTC alleges that, at least since April 2008, Wyndham engaged in unfair cybersecurity practices that, "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." This claim is fleshed out as follows.

> 1. The company allowed Wyndham-branded hotels to store payment card information in clear readable text.
>
> 2. Wyndham allowed the use of easily guessed passwords to access the property management systems. For example, to gain "remote access to at least one hotel's system," which was developed by Micros Systems, Inc., the user ID and password were both "micros."
>
> 3. Wyndham failed to use "readily available security measures"—such as firewalls—to "limit access between [the] hotels' property management systems, . . . corporate network, and the Internet."
>
> 4. Wyndham allowed hotel property management systems to connect to its network without taking appropriate cybersecurity precautions. It did not ensure that the hotels implemented "adequate information security policies and

> procedures." Also, it knowingly allowed at least one hotel to connect to the Wyndham network with an out-of-date operating system that had not received a security update in over three years. It allowed hotel servers to connect to Wyndham's network even though "default user IDs and passwords were enabled . . . , which were easily available to hackers through simple Internet searches." And, because it failed to maintain an "adequate[] inventory [of] computers connected to [Wyndham's] network [to] manage the devices," it was unable to identify the source of at least one of the cybersecurity attacks.
>
> 5. Wyndham failed to "adequately restrict" the access of third-party vendors to its network and the servers of Wyndham-branded hotels. For example, it did not "restrict[] connections to specified IP addresses or grant[] temporary, limited access, as necessary."
>
> 6. It failed to employ "reasonable measures to detect and prevent unauthorized access" to its computer network or to "conduct security investigations."
>
> 7. It did not follow "proper incident response procedures." The hackers used similar methods in each attack, and yet Wyndham failed to monitor its network for malware used in the previous intrusions.

Although not before us on appeal, the complaint also raises a deception claim, alleging that since 2008 Wyndham has published a privacy policy on its website that overstates the company's cybersecurity.

> We safeguard our Customers' personally identifiable information by using industry standard practices. Although "guaranteed security" does not exist either on or off the Internet, we make commercially reasonable efforts to make our collection of such [i]nformation consistent with all applicable laws and regulations. Currently, our Web sites utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by Verisign Inc. This allows for utilization of Secure Sockets Layer, which is a method for encrypting data. This protects confidential information—such as credit card numbers, online forms, and financial data—from loss, misuse, interception, and hacking. We take commercially reasonable efforts to create and maintain "fire walls" and other appropriate safeguards . . . .

The FTC alleges that, contrary to this policy, Wyndham did not use encryption, firewalls, and other commercially reasonable methods for protecting consumer data.

As noted, on three occasions in 2008 and 2009 hackers accessed Wyndham's network and the property management systems of Wyndham-branded hotels. In April 2008, hackers first broke into the local network of a hotel in Phoenix, Arizona, which was connected to Wyndham's network and the Internet. They then used the brute-force method—repeatedly guessing users' login IDs and passwords—to access an administrator account on Wyndham's network. This enabled them to obtain consumer data on computers throughout the network. In total, the hackers obtained unencrypted information for over 500,000 accounts, which they sent to a domain in Russia.

In March 2009, hackers attacked again, this time by accessing Wyndham's network through an administrative account. The FTC claims that Wyndham was unaware of the attack for two months until consumers filed complaints about fraudulent charges. Wyndham then discovered "memory-scraping malware" used in the previous attack on more than thirty hotels' computer systems. The FTC asserts that, due to Wyndham's "failure to monitor [the network] for the malware used in the previous attack, hackers had unauthorized access to [its] network

for approximately two months." In this second attack, the hackers obtained unencrypted payment card information for approximately 50,000 consumers from the property management systems of 39 hotels.

Hackers in late 2009 breached Wyndham's cybersecurity a third time by accessing an administrator account on one of its networks. Because Wyndham "had still not adequately limited access between . . . the Wyndham-branded hotels' property management systems, [Wyndham's network], and the Internet," the hackers had access to the property management servers of multiple hotels. Wyndham only learned of the intrusion in January 2010 when a credit card company received complaints from cardholders. In this third attack, hackers obtained payment card information for approximately 69,000 customers from the property management systems of 28 hotels.

The FTC alleges that, in total, the hackers obtained payment card information from over 619,000 consumers, which (as noted) resulted in at least $10.6 million in fraud loss. It further states that consumers suffered financial injury through "unreimbursed fraudulent charges, increased costs, and lost access to funds or credit," and that they "expended time and money resolving fraudulent charges and mitigating subsequent harm."

The Federal Trade Commission Act of 1914 prohibited "unfair methods of competition in commerce." Congress "explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' . . . by enumerating the particular practices to which it was intended to apply." The takeaway is that Congress designed the term as a "flexible concept with evolving content," and "intentionally left [its] development . . . to the Commission."

After several early cases limited "unfair methods of competition" to practices harming competitors and not consumers, Congress inserted an additional prohibition in § 45(a) against "unfair or deceptive acts or practices in or affecting commerce."

In 1994, Congress codified the 1980 Policy Statement at 15 U.S.C. § 45(n):

> The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

Wyndham argues . . . that the three requirements of 15 U.S.C. § 45(n) are necessary but insufficient conditions of an unfair practice and that the plain meaning of the word “unfair” imposes independent requirements that are not met here. [C]iting one dictionary, Wyndham argues that a practice is only "unfair" if it is "not equitable" or is "marked by injustice, partiality, or deception." Whether these are requirements of an unfairness claim makes little difference here. A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.

We recognize this analysis of unfairness encompasses some facts relevant to the FTC's deceptive practices claim. But facts relevant to unfairness and deception claims frequently overlap. We cannot completely disentangle the two theories here. The FTC argued in the District Court that consumers could not reasonably avoid injury by booking with another hotel chain because Wyndham had published a misleading privacy policy that overstated its

cybersecurity. Wyndham did not challenge this argument in the District Court nor does it do so now. If Wyndham's conduct satisfies the reasonably avoidable requirement at least partially because of its privacy policy—an inference we find plausible at this stage of the litigation—then the policy is directly relevant to whether Wyndham's conduct was unfair.

Finally, Wyndham posits a *reductio ad absurdum*, arguing that if the FTC's unfairness authority extends to Wyndham's conduct, then the FTC also has the authority to "regulate the locks on hotel room doors, . . . to require every store in the land to post an armed guard at the door," and to sue supermarkets that are "sloppy about sweeping up banana peels." The argument is alarmist to say the least. And it invites the tart retort that, were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a).

We are therefore not persuaded by Wyndham's arguments that the alleged conduct falls outside the plain meaning of "unfair."

Wyndham next argues that, even if cybersecurity were covered by § 45(a) as initially enacted, three legislative acts since the subsection was amended in 1938 have reshaped the provision's meaning to exclude cybersecurity. A recent amendment to the Fair Credit Reporting Act directed the FTC and other agencies to develop regulations for the proper disposal of consumer data. The Gramm–Leach–Bliley Act required the FTC to establish standards for financial institutions to protect consumers' personal information. And the Children's Online Privacy Protection Act ordered the FTC to promulgate regulations requiring children's websites, among other things, to provide notice of "what information is collected from children . . . , how the operator uses such information, and the operator's disclosure practices for such information." Wyndham contends these "tailored grants of substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general substantive authority over this field." Citing *FDA v. Brown & Williamson Tobacco Corp. (2000)*, Wyndham concludes that Congress excluded cybersecurity from the FTC's unfairness authority by enacting these measures.

We are not persuaded. The Fair Credit Reporting Act requires (rather than authorizes) the FTC to issue regulations and expands the scope of the FTC's authority ("[A] violation of any requirement or prohibition imposed under this subchapter shall constitute an unfair or deceptive act or practice in commerce . . . and shall be subject to enforcement by the [FTC] . . . irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests under the [FTC] Act."). The Gramm–Leach–Bliley Act similarly requires the FTC to promulgate regulations and relieves some of the burdensome § 45(n) requirements for declaring acts unfair ("[The FTC] shall establish appropriate standards . . . to protect against unauthorized access to or use of . . . records . . . which could result in substantial harm *or inconvenience to any customer*."). And the Children's Online Privacy Protection Act required the FTC to issue regulations and empowered it to do so under the procedures of the Administrative Procedure Act, rather than the more burdensome Magnuson–Moss procedures under which the FTC must usually issue regulations. Thus, none of the recent privacy legislation was "inexplicable" if the FTC already had some authority to regulate corporate cybersecurity through § 45(a).

Having rejected Wyndham's arguments that its conduct cannot be unfair, we assume for the remainder of this opinion that it was.

A conviction or punishment violates the Due Process Clause of our Constitution if the statute or regulation under which it is obtained "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *FCC v. Fox Television Stations* (2012). Wyndham claims that, notwithstanding whether its conduct was unfair under § 45(a), the FTC failed to give fair notice of the specific cybersecurity standards the company was required to follow.

The level of required notice for a person to be subject to liability varies by circumstance. In *Bouie v. City of Columbia* (1964), the Supreme Court held that a "judicial construction of a criminal statute" violates due process if it is "unexpected and indefensible by reference to the law which had been expressed prior to the conduct in issue." The precise meaning of "unexpected and indefensible" is not entirely clear, but we and our sister circuits frequently use language implying that a conviction violates due process if the defendant could not reasonably foresee that a court might adopt the new interpretation of the statute. The fair notice doctrine extends to civil cases, particularly where a penalty is imposed.

[T]he relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute. If later proceedings in this case develop such that the proper resolution is to defer to an agency interpretation that gives rise to Wyndham's liability, we leave to that time a fuller exploration of the level of notice required. For now, however, it is enough to say that we accept Wyndham's forceful contention that we are interpreting the FTC Act (as the District Court did). As a necessary consequence, Wyndham is only entitled to notice of the meaning of the statute and not to the agency's interpretation of the statute.

Having decided that Wyndham is entitled to notice of the meaning of the statute, we next consider whether the case should be dismissed based on fair notice principles. We do not read Wyndham's briefs as arguing the company lacked fair notice that cybersecurity practices can, as a general matter, form the basis of an unfair practice under § 45(a). Wyndham argues instead it lacked notice of what *specific* cybersecurity practices are necessary to avoid liability. We have little trouble rejecting this claim.

To begin with, Wyndham's briefing focuses on the FTC's failure to give notice of its interpretation of the statute and does not meaningfully argue that the statute itself fails fair notice principles. We think it imprudent to hold a 100-year-old statute unconstitutional as applied to the facts of this case when we have not expressly been asked to do so.

In this context, the relevant legal rule is not "so vague as to be 'no rule or standard at all.'" Subsection 45(n) asks whether "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." While far from precise, this standard informs parties that the relevant inquiry here is a cost-benefit analysis, that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity. We acknowledge there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls. Fair notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute.

What appears to us is that Wyndham's fair notice claim must be reviewed as an as-applied challenge. Yet Wyndham does not argue that its cybersecurity practices survive a reasonable interpretation of the cost-benefit analysis required by § 45(n). One sentence in Wyndham's reply brief says that its "view of what data-security practices are unreasonable . . . is not necessarily the same as the FTC's." Too little and too late.

Wyndham's as-applied challenge falls well short given the allegations in the FTC's complaint. As the FTC points out in its brief, the complaint does not allege that Wyndham used *weak* firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use *any* firewall at critical network points, did not restrict specific IP addresses *at all,* did not use *any* encryption for certain customer files, and did not require some

users to change their default or factory-setting passwords *at all*. Wyndham did not respond to this argument in its reply brief.

Wyndham's as-applied challenge is even weaker given it was hacked not one or two, but three, times. At least after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis. That said, we leave for another day whether Wyndham's alleged cybersecurity practices do in fact fail, an issue the parties did not brief. We merely note that certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court *could* find that its practices fail the cost-benefit analysis.

Several other considerations reinforce our conclusion that Wyndham's fair notice challenge fails. In 2007 the FTC issued a guidebook, *Protecting Personal Information: A Guide for Business*, which describes a "checklist[]" of practices that form a "sound data security plan." The guidebook does not state that any particular practice is required by § 45(a), but it does counsel against many of the specific practices alleged here. For instance, it recommends that companies "consider encrypting sensitive information that is stored on [a] computer network . . . [, c]heck . . . software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches." It recommends using "a firewall to protect [a] computer from hacker attacks while it is connected to the Internet," deciding "whether [to] install a 'border' firewall where [a] network connects to the Internet," and setting access controls that "determine who gets through the firewall and what they will be allowed to see . . . to allow only trusted employees with a legitimate business need to access the network." It recommends "requiring that employees use 'strong' passwords" and cautions that "[h]ackers will first try words like . . . the software's default password[] and other easy-to-guess choices." And it recommends implementing a "breach response plan," which includes "[i]nvestigat[ing] security incidents immediately and tak[ing] steps to close off existing vulnerabilities or threats to personal information."

As the agency responsible for administering the statute, the FTC's expert views about the characteristics of a "sound data security plan" could certainly have helped Wyndham determine in advance that its conduct might not survive the cost-benefit analysis.

Before the attacks, the FTC also filed complaints and entered into consent decrees in administrative cases raising unfairness claims based on inadequate corporate cybersecurity. The agency published these materials on its website and provided notice of proposed consent orders in the Federal Register. Wyndham responds that the complaints cannot satisfy fair notice principles because they are not "adjudications on the merits." But even where the "ascertainable certainty" standard applies to fair notice claims, courts regularly consider materials that are neither regulations nor "adjudications on the merits." That the FTC commissioners—who must vote on whether to issue a complaint—believe that alleged cybersecurity practices fail the cost-benefit analysis of § 45(n) certainly helps companies with similar practices apprehend the possibility that their cybersecurity could fail as well.

In sum, we have little trouble rejecting Wyndham's fair notice claim.

Notes

1. If one compares Wyndham's conduct to the data security guidelines, many shortcomings are obvious. This is fairly typical in data breach cases. Most data breaches that attract FTC notice are the result of numerous failures of data security rather than just one.

Consider how issues of fair notice play into the LabMD case. Does the court's reasoning there suggest a problem with *Wyndham*?

LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018)

TJOFLAT, Circuit Judge:

This is an enforcement action brought by the Federal Trade Commission ("FTC" or "Commission") against LabMD, Inc., alleging that LabMD's data-security program was inadequate and thus constituted an "unfair act or practice" under Section 5(a) of the Federal Trade Commission Act (the "FTC Act" or "Act"), 15 U.S.C. § 45(a). Following a trial before an administrative law judge ("ALJ"), the Commission issued a cease-and-desist order directing LabMD to create and implement a variety of protective measures. LabMD petitions this Court to vacate the order, arguing that the order is unenforceable because it does not direct LabMD to cease committing an unfair act or practice within the meaning of Section 5(a). We agree and accordingly vacate the order.

LabMD is a now-defunct medical laboratory that previously conducted diagnostic testing for cancer.[3] It used medical specimen samples, along with relevant patient information, to provide physicians with diagnoses. Given the nature of its work, LabMD was subject to data-security regulations issued under the Health Insurance Portability and Accountability Act of 1996, known colloquially as HIPAA. LabMD employed a data-security program in an effort to comply with those regulations.

Sometime in 2005, contrary to LabMD policy, a peer-to-peer file-sharing application called LimeWire was installed on a computer used by LabMD's billing manager. LimeWire is an application commonly used for sharing and downloading music and videos over the Internet. It connects to the "Gnutella" network, which during the relevant period had two to five million people logged in at any given time. Those using LimeWire and connected to the Gnutella network can browse directories and download files that other users on the network designate for sharing. The billing manager designated the contents of the "My Documents" folder on her computer for sharing, exposing the contents to the other users. Between July 2007 and May 2008, this folder contained a 1,718-page file (the "1718 File") with the personal information of 9,300 consumers, including names, dates of birth, social security numbers, laboratory test codes, and, for some, health insurance company names, addresses, and policy numbers.

In February 2008, Tiversa Holding Corporation, an entity specializing in data security, used LimeWire to download the 1718 File. Tiversa began contacting LabMD months later, offering to sell its remediation services to LabMD. LabMD refused Tiversa's services and removed LimeWire from the billing manager's computer. Tiversa's solicitations stopped in July 2008, after LabMD instructed Tiversa to direct any further communications to LabMD's lawyer. In 2009, Tiversa arranged for the delivery of the 1718 File to the FTC.

In August 2013, the Commission, following an extensive investigation, issued an administrative complaint against LabMD and assigned an ALJ to the case. The complaint alleged that LabMD had committed an "unfair act or practice" prohibited by Section 5(a) by "engag[ing] in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks." Rather than allege specific acts or practices that LabMD engaged in, however, the FTC's complaint set forth a number of data-security measures that LabMD failed to perform. LabMD answered the complaint, denying it had engaged in the conduct alleged and asserting several affirmative defenses, among them that the Commission lacked authority under Section 5 of the Act to regulate its handling of the personal information in its computer networks.

Next, the Commission addressed and rejected LabMD's arguments that Section 5(a)'s "unfairness" standard—which, according to the Commission, is a reasonableness standard—is void for vagueness and that the Commission failed to provide fair notice of what data-security

[3] LabMD is no longer in operation but still exists as a company and continues to secure its computers and the patient data stored within them.

practices were adequate under Section 5(a). The FTC then entered an order vacating the ALJ's decision and enjoining LabMD to install a data-security program that comported with the FTC's standard of reasonableness. The order is to terminate on either July 28, 2036, or twenty years "from the most recent date that the [FTC] files a complaint . . . in federal court alleging any violation of the order, whichever comes later."

LabMD petitioned this Court to review the FTC's decision. LabMD then moved to stay enforcement of the FTC's cease-and-desist order pending review, arguing that compliance with the order was unfeasible given LabMD's defunct status and *de minimis* assets.

Now, LabMD argues that the Commission's cease-and-desist order is unenforceable because the order does not direct it to cease committing an unfair "act or practice" within the meaning of Section 5(a).

Section 5(a) of the FTC Act authorizes the FTC to protect consumers by "prevent[ing] persons, partnerships, or corporations . . . from using unfair . . . acts or practices in or affecting commerce." The Act does not define the term "unfair." The provision's history, however, elucidates the term's meaning.

The FTC Act, passed in 1914, created the FTC and gave it power to prohibit "unfair methods of competition." Rather than list "the particular practices to which [unfairness] was intended to apply," Congress "intentionally left development of the term 'unfair' to the Commission" through case-by-case litigation—though, at the time of the FTC Act's inception, the FTC's primary mission was understood to be the enforcement of antitrust law. In 1938, the Act was amended to provide that the FTC had authority to prohibit "unfair . . . acts or practices." This amendment sought to clarify that the FTC's authority applied not only to competitors but, importantly, also to consumers. Hence, the FTC possesses "unfairness authority" to prohibit and prosecute unfair acts or practices harmful to consumers.

Here, the FTC's complaint alleges that LimeWire was installed on the computer used by LabMD's billing manager. This installation was contrary to company policy. The complaint then alleges that LimeWire's installation caused the 1718 File, which consisted of consumers' personal information, to be exposed. The 1718 File's exposure caused consumers injury by infringing upon their right of privacy. Thus, the complaint alleges that LimeWire was installed in defiance of LabMD policy and caused the alleged consumer injury. Had the complaint stopped there, a narrowly drawn and easily enforceable order might have followed, commanding LabMD to eliminate the possibility that employees could install unauthorized programs on their computers.

But the complaint continues past this single allegation of wrongdoing, adding that LimeWire's installation was not the only conduct that caused the 1718 File to be exposed. It also alleges broadly that LabMD "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks." The complaint then provides a litany of security measures that LabMD failed to employ, each setting out in general terms a deficiency in LabMD's data-security protocol. Because LabMD failed to employ these measures, the Commission's theory goes, LimeWire was able to be installed on the billing manager's computer. LabMD's policy forbidding employees from installing programs like LimeWire was insufficient.

The FTC's complaint, therefore, uses LimeWire's installation, and the 1718 File's exposure, as an entry point to broadly allege that LabMD's data-security operations are deficient as a whole. Aside from the installation of LimeWire on a company computer, the complaint alleges no specific unfair acts or practices engaged in by LabMD. Rather, it was LabMD's multiple, unspecified failures to act in creating and operating its data-security program that amounted to an unfair act or practice. Given the breadth of these failures, the Commission attached to its complaint a proposed order which would regulate all aspects of LabMD's data-security program—sweeping prophylactic measures to collectively reduce the

possibility of employees installing unauthorized programs on their computers and thus exposing consumer information. The proposed cease-and-desist order, which is identical in all relevant respects to the order the FTC ultimately issued, identifies no specific unfair acts or practices from which LabMD must abstain and instead requires LabMD to implement and maintain a data-security program "reasonably designed" to the Commission's satisfaction.

The first question LabMD's petition for review presents is whether LabMD's failure to implement and maintain a reasonably designed data-security program constituted an unfair act or practice within the ambit of Section 5(a). The FTC declared that it did because such failure caused substantial injury to consumers' right of privacy, and it issued a cease-and-desist order to avoid further injury.

The Commission must find the standards of unfairness it enforces in "clear and well-established" policies that are expressed in the Constitution, statutes, or the common law. The Commission's decision in this case does not explicitly cite the source of the standard of unfairness it used in holding that LabMD's failure to implement and maintain a reasonably designed data-security program constituted an unfair act or practice. It is apparent to us, though, that the source is the common law of negligence. According to the Restatement (Second) of Torts § 281 (Am. Law Inst. 1965), Statement of the Elements of a Cause of Action for Negligence,

> [an] actor is liable for an invasion of an interest of another, if:
>
> (a) the interest invaded is protected against unintentional invasion, and
>
> (b) the conduct of the actor is negligent with respect to the other, or a class of persons within which [the other] is included, and
>
> (c) the actor's conduct is a legal cause of the invasion, and
>
> (d) the other has not so conducted himself as to disable himself from bringing an action for such invasion.

The gist of the Commission's complaint and its decision is this: The consumers' right of privacy is protected against unintentional invasion. LabMD unintentionally invaded their right, and its deficient data-security program was a legal cause. Section 5(a) empowers the Commission to "prevent persons, partnerships, or corporations . . . from using unfair . . . acts or practices." The law of negligence, the Commission's action implies, is a source that provides standards for determining whether an act or practice is unfair, so a person, partnership, or corporation that negligently infringes a consumer interest protected against unintentional invasion may be held accountable under Section 5(a). We will assume *arguendo* that the Commission is correct and that LabMD's negligent failure to design and maintain a reasonable data-security program invaded consumers' right of privacy and thus constituted an unfair act or practice.

The second question LabMD's petition for review presents is whether the Commission's cease-and-desist order, founded upon LabMD's general negligent failure to act, is enforceable. We answer this question in the negative. We illustrate why by first laying out the FTC Act's enforcement and remedial schemes and then by demonstrating the problems that enforcing the order would pose.

Under Section 5(*l*), the Commission may bring a civil-penalty action in district court should the respondent violate a final cease-and-desist order. The Commission's complaint would allege that the defendant is subject to an existing cease-and-desist order and has violated its terms. For each separate violation of the order—or, in the case of a continuing violation, for each day in violation—the district court may impose a penalty of up to $41,484. Section 5(*l*) also empowers the district court to grant an injunction if the Commission proves that the violation is likely to continue and an injunction is necessary to enforce the order.

If the Commission has obtained an injunction in district court requiring the defendant to discontinue an unfair act or practice, it may invoke the district court's civil-contempt power should the defendant disobey. Rather than filing a complaint, as in a Section 5(*l*) action, the Commission simply moves the district court for an order requiring the defendant to show cause why it should not be held in contempt for engaging in conduct the injunction specifically enjoined.

The concept of specificity is crucial to both modes of enforcement. We start with civil penalties for violations of cease-and-desist orders. Nothing in the FTC Act addresses what content must go into a cease-and-desist order. The FTC Rule of Practice governing Commission complaints, however, states that a complaint must contain "[a] clear and concise factual statement sufficient to inform each respondent with reasonable definiteness of the type of acts or practices alleged to be in violation of the law." It follows that the remedy the complaint seeks must comport with this requirement of reasonable definiteness. Moreover, given the severity of the civil penalties a district court may impose for the violation of a cease-and-desist order, the order's prohibitions must be stated with clarity and precision. The United States Supreme Court emphasized this point in *FTC v. Colgate-Palmolive Co.* (1965), stating,

> [T]his Court has . . . warned that an order's prohibitions should be clear and precise in order that they may be understood by those against whom they are directed, and that [t]he severity of possible penalties prescribed . . . for violations of orders which have become final underlines the necessity for fashioning orders which are, at the outset, sufficiently clear and precise to avoid raising serious questions as to their meaning and application.

The imposition of penalties upon a party for violating an imprecise cease-and-desist order—up to $41,484 per violation or day in violation—may constitute a denial of due process.

Specificity is equally important in the fashioning and enforcement of an injunction consequent to an action brought in district court under Section 13(b). Indeed, "[t]he most fundamental postulates of our legal order forbid the imposition of a penalty for disobeying a command that defies comprehension." *Int'l Longshoremen's Ass'n, Local 1291 v. Phila. Marine Trade Ass'n* (1967). Being held in contempt and sanctioned pursuant to an insufficiently specific injunction is therefore a denial of due process.

In sum, the prohibitions contained in cease-and-desist orders and injunctions must be specific. Otherwise, they may be unenforceable. Both coercive orders are also governed by the same standard of specificity, as the stakes involved for a violation are the same—severe penalties or sanctions.

In the case at hand, the cease-and-desist order contains no prohibitions. It does not instruct LabMD to stop committing a specific act or practice. Rather, it commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness. This command is unenforceable. Its unenforceability is made clear if we imagine what would take place if the Commission sought the order's enforcement. As we have explained, the standards a district court would apply are essentially the same whether it is entertaining the Commission's action for the imposition of a penalty or the Commission's motion for an order requiring the enjoined defendant to show cause why it should not be adjudicated in contempt. For ease of discussion, we posit a scenario in which the Commission obtained the coercive order it entered in this case from a district court, and now seeks to enforce the order.

The Commission moves the district court for an order requiring LabMD to show cause why it should not be held in contempt for violating the following injunctive provision:

> [T]he respondent shall . . . establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information

> collected from or about consumers . . . . Such program . . . shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers . . . .

The Commission's motion alleges that LabMD's program failed to implement "*x*" and is therefore not "reasonably designed." The court concludes that the Commission's alleged failure is within the provision's language and orders LabMD to show cause why it should not be held in contempt.

At the show cause hearing, LabMD calls an expert who testifies that the data-security program LabMD implemented complies with the injunctive provision at issue. The expert testifies that "*x*" is not a necessary component of a reasonably designed data-security program. The Commission, in response, calls an expert who disagrees. At this point, the district court undertakes to determine which of the two equally qualified experts correctly read the injunctive provision. Nothing in the provision, however, indicates which expert is correct. The provision contains no mention of "*x*" and is devoid of any meaningful standard informing the court of what constitutes a "reasonably designed" data-security program. The court therefore has no choice but to conclude that the Commission has not proven—and indeed cannot prove—LabMD's alleged violation by clear and convincing evidence.

If the court held otherwise and ordered LabMD to implement "*x*," the court would have effectively modified the injunction at a show cause hearing. This would open the door to future modifications, all improperly made at show cause hearings.

The practical effect of repeatedly modifying the injunction at show cause hearings is that the district court is put in the position of managing LabMD's business in accordance with the Commission's wishes. It would be as if the Commission was LabMD's chief executive officer and the court was its operating officer. It is self-evident that this micromanaging is beyond the scope of court oversight contemplated by injunction law.

In sum, assuming *arguendo* that LabMD's negligent failure to implement and maintain a reasonable data-security program constituted an unfair act or practice under Section 5(a), the Commission's cease-and-desist order is nonetheless unenforceable. It does not enjoin a specific act or practice. Instead, it mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished. Moreover, it effectually charges the district court with managing the overhaul. This is a scheme Congress could not have envisioned.

Notes

1. Pre-*LabMD*, FTC orders were both vague and nearly identical. Specifically, orders for a variety of defendants had variants of the following language:

   > IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing products and services for consumers, and (2) protect the security, integrity, and confidentiality of covered information, whether collected by respondent or input into, stored on, captured with, or accessed through a computer using respondent's products or services.

   This appeared, for instance, in the 2014 consent decree with Fandango. The subsequent paragraphs in the order, quoted in part in the *LabMD* case, shed little additional light on exactly what is required. FTC orders post-*LabMD* have gotten more specific, resembling checklists. Consider the 2019 Equifax order. The word "reasonable" all but disappears.

"Regular" penetration testing is replaced with "once every twelve months." Equifax needed a system in place for employee security complaints by August 30, 2019 (about a month from the issue date). There were also a series of specific requirements:

> Establishing patch management policies and procedures that require confirmation that any directives to apply patches or remediate vulnerabilities are received and completed . . . ;
>
> Identifying and documenting a comprehensive information technology ("IT") asset inventory that includes hardware, software, and location of the assets;
>
> Designing and implementing protections such as network intrusion protection, host intrusion protection, and file integrity monitoring . . . ;
>
> Designing, implementing, and maintaining measures to limit unauthorized access in any network or system that stores, collects, maintains, or processes Personal Information, such as segmentation of networks and databases and properly configured firewalls;
>
> Implementing access controls across Defendant's network, such as multi-factor authentication and strong password requirements;
>
> Limiting user access privileges to systems that provide access to Personal Information to employees, contractors, or other authorized third parties with a business need to access such information and establishing regular documented review of such access privileges;
>
> Establishing regular information security training programs, updated, as applicable, to address internal or external risks identified by Defendant, including, at a minimum: At least annual information security awareness training for all employees . . .

It is unclear to what extent these data security requirements will evolve over time. Do these additional requirements address the *LabMD* concerns?

2. Recall from health privacy: HIPAA does not have a private right of action, but courts sometimes use HIPAA to establish the standard of care for private lawsuits based on the duty of confidentiality or negligence. Similarly, courts sometimes cite to Section 5 in data security cases. For instance:

> Plaintiffs allege that Equifax violated Section 5 of the FTC Act, and similar state statutes, by "failing to use reasonable measures to protect Personal Information and not complying with industry standards," and that such violation constitutes negligence per se. "Georgia law allows the adoption of a statute or regulation as a standard of conduct so that its violation becomes negligence per se." In order to make a negligence per se claim, however, the plaintiff must show that it is within the class of persons intended to be protected by the statute and that the statute was meant to protect against the harm suffered.
>
> [In *LabMD*, the court] did not hold that inadequate data security cannot be regulated under Section 5. Next, the Defendants argue that the Plaintiffs have not sufficiently alleged injury or proximate causation. Under Georgia law, negligence per se is "not liability per se." Even if negligence per se is shown, a plaintiff must still prove proximate causation and actual damage to recover. As discussed above, the Court concludes that the Plaintiffs have sufficiently alleged both a legally cognizable injury and proximate causation. Therefore, this argument is unavailing.

In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F.Supp.3d 1295, 1327 (N.D. Ga. 2019). Notably, the negligence per se cause of action does not get around the difficult questions of injury and causation.

In the Matter of Chegg, Inc. (FTC 2023)

Complaint

The Federal Trade Commission, having reason to believe that Chegg, Inc., a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

Chegg markets and sells direct-to-student educational products and services. Its "Required Materials" service includes selling and renting textbooks to students. Its "Chegg Services" products and services include online learning aids, such as online tutoring, writing assistance, a math-problem solver, and answers to common textbook questions. Chegg has asserted that the target audience for its services are primarily high school and college students.

In providing its services, Chegg collects sensitive personal information from users. For example, in connection with its scholarship search service, Chegg has collected information about a user's religious denomination, heritage, date of birth, parents' income range, sexual orientation, and disabilities (collectively, the "Scholarship Search Data"). In a 2018 internal email, Chegg's employee in charge of cybersecurity described the Scholarship Search Data as "very sensitive."

As another example, in connection with its online tutoring services, Chegg recorded videos of tutoring sessions that included Chegg users' images and voices.

Chegg has also collected sensitive personal information from its employees in the course of employment. This includes employees' names, dates of birth, Social Security numbers, and financial information.

As part of its information technology infrastructure, Chegg uses a third-party service provided by Amazon Web Services called the Simple Storage Service ("S3"). S3 is a scalable cloud storage service that can be used to store and retrieve large amounts of data. The S3 stores data inside virtual containers, called "buckets," against which individual access controls can be applied.

Chegg relies on S3 buckets to store a wide variety of files that contain users' sensitive personal information, including their names, passwords, dates of birth, and Scholarship Search Data (collectively, the "S3 User Data").

From at least 2017 to the present, Chegg has engaged in a number of practices that, taken individually or together, failed to provide reasonable security to prevent unauthorized access to users' personal information. These shortcomings also failed to provide reasonable security for the personal information Chegg collects from its employees, which has similarly resulted in unauthorized access to that information. Among other things, Chegg:

a) failed to implement reasonable access controls to safeguard users' personal information stored in S3 databases until at earliest October 2018. Specifically, Chegg:

   i) failed to require employees and third-party contractors that access the S3 databases to use distinct access keys, instead permitting employees and contractors to use a single AWS access key that provided full administrative privileges over all data in the S3 databases ("AWS Root Credentials");

   ii) failed to restrict access to systems based on employees' or contractors' job functions;

   iii) failed to require multi-factor authentication for account access to the S3 databases; and

iv) failed to rotate access keys to the S3 databases;

b) stored users' and employees' personal information on Chegg's network and databases, including S3 databases, in plain text, rather than encrypting the information;

c) used, until at least April 2018, outdated and unsecure cryptographic hash functions to protect users' passwords;

d) failed, until January 2021, to develop, implement, or maintain adequate written organizational information security standards, policies, procedures, or practices;

e) failed, until at earliest April 2020, to provide adequate guidance or training for employees or third-party contractors regarding information security and safeguarding users' and employees' personal information, including, but not limited to, failing to require employees to complete any data security training;

f) failed to have a policy, process, or procedure for inventorying and deleting users' and employees' personal information stored on Chegg's network after that information is no longer necessary; and

g) failed to adequately monitor its networks and systems for unauthorized attempts to transfer or exfiltrate users' and employees' personal information outside of Chegg's network boundaries.

Chegg's failure to provide reasonable security for the personal information it collected from users and employees has led to the repeated exposure of that personal information.

In or around September 2017, Chegg employees fell for a phishing attack, giving the threat actors access to employees' direct deposit information. Prior to the hack, Chegg did not require employees to complete any data security training, including identifying and appropriately responding to phishing attacks; this failure contributed to the security incident.

In or around April 2018, a former contractor accessed one of Chegg's S3 databases using an AWS Root Credential. Although Amazon had provided public guidance to protect AWS Root Credentials "like you would your credit card numbers or any other sensitive secret" and that Amazon "strongly recommend[s] that you do not use the root user for your everyday tasks, even the administrative ones," Chegg shared the AWS Root Credentials among its employees and even outside contractors. Using the AWS Root Credentials, the former contractor exfiltrated a database containing personal information of approximately 40 million users of the Chegg platform. The exposed personal information included the S3 User Data consisting of users' email addresses, first and last names, passwords, and, for certain Chegg users, their Scholarship Search Data, consisting of their religious denomination, heritage, date of birth, parents' income range, sexual orientation, and disabilities.

In September 2018, a threat intelligence vendor informed Chegg that a file containing some of the exfiltrated information was available in an online forum. Chegg reviewed the file as part of its own investigation, finding it held, among other things, approximately 25 million of the exfiltrated passwords in plain text, meaning the threat actors had cracked the hash for those passwords. Chegg required approximately 40 million Chegg platform users to reset their passwords. And, while Chegg implemented some access controls—rotating credentials and creating credentials with access permissions tailored to an employee's job functions—it failed to address, and allowed to persist, the remaining data securities failures . . . .

In or around April 2019, a senior Chegg executive fell victim to a phishing attack, giving the threat actor access to the executive's credentials to Chegg's email platform and exposing personal information about consumers and employees of Chegg. This executive's email system was in a default configuration state that allowed employees, as well as threat actors, to bypass Chegg's multifactor authentication requirement while accessing the email platform.

In or around April 2020, Chegg's senior employee responsible for payroll fell victim to a phishing attack, giving the threat actor access to the employee's credentials to Chegg's payroll system. The threat actor exfiltrated the W-2 information, including the birthdates and Social Security numbers, of approximately 700 current and former employees.

Injury to Consumers

The information collected by Chegg, including users' and employees' medical conditions and financial information, together with identifying information such as their names, email addresses, passwords, birthdates, and Social Security numbers, is highly sensitive.

Chegg's failure to provide reasonable security for users' and employees' personal information has caused or is likely to cause substantial injury to those users and employees in the form of fraud, identity theft, monetary loss, stigma, embarrassment, emotional distress, and time spent remedying or attempting to prevent any of these potential injuries.

Even if identity theft and fraud do not occur immediately after a breach, a breach of personal information such as that stored in Chegg's system makes identity theft and fraud more likely in the future.

Furthermore, due to Chegg's failure to appropriately monitor its systems and lack of access controls and authentication protections for its S3 databases, users' and employees' personal information, including health information and financial information, may have been exposed in other instances . . . without Chegg's knowledge.

The harms . . . were not reasonably avoidable by users or employees, as users had no way to know about Chegg's information security shortcomings.

Further, the harms are not outweighed by any countervailing benefits to users or competition. Chegg could have prevented or mitigated these information security failures through readily available, and relatively low-cost, measures. For example, as part of its AWS service, Amazon offers server-side encryption that encrypts data at rest (such as the S3 User Data) using encryption keys managed by Amazon.

Chegg's Deceptive Security Statements

From at least March 2017 to January 2020, Chegg disseminated, or caused to be disseminated, a privacy policy that expressly applied to Chegg's websites, apps, and other services. During this time period, the privacy policy contained the following claim regarding the security measures Chegg used to protect the personal information it collected from users: "Chegg takes commercially reasonable security measures to protect the Personal Information submitted to us, both during transmission and once we receive it."

From January 2020 to the present, Chegg's privacy policy contained the following statement concerning that same personal information: "We take steps to ensure that your information is treated securely and in accordance with this Privacy Policy."

Count I - Unfair Data Security Practices

Chegg's failure to employ reasonable and appropriate measures to protect personal information caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.

Count II - Data Security Misrepresentations

Chegg has represented, directly or indirectly, expressly or by implication, that it implemented reasonable measures to protect personal information against unauthorized access.

In fact, . . . Chegg did not implement reasonable measures to protect personal information against unauthorized access. Therefore, the representation [set forth in the previous paragraph] is false or misleading.

Notes

1. Chegg settled this case in January 2023. The FTC's order requires Chegg to implement a comprehensive information security program, limit the data the company can collect and retain, offer users multifactor authentication to secure their accounts, and allow users to request access to and deletion of their data.
2. Chegg is a prototypical FTC data security enforcement action. The FTC brings actions against companies that have repeated or egregious failures of data security. These failures will generally involve networks with poor external security, phishing schemes, and overly broad employee access to data. In settlement, the FTC will require broadly better data security, particularly multifactor authentication, limiting employee access to payment information, and re-training employees to raise awareness of phishing scams and similar data security risks.
3. Not every FTC data security enforcement action is about payment information and other easily monetizable data. In 2014, the FTC brought suit against and settled with TRENDnet for security problems in its line of home security cameras.[226] TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring, and claimed in numerous product descriptions that they were "secure." Though users were supposed to be able to designate camera feeds as public (viewable by anyone) or private (viewable only with password/authentication), it was sometimes possible for people to access even private cameras if they had the camera's internet address. In total, hackers posted links to about 700 live feeds from supposedly private cameras. In settlement, TRENDnet agreed to notify customers about the security issues with the cameras and the availability of a software update to correct them, and to provide customers with free technical support for the next two years to assist them in updating or uninstalling their cameras.

[226] Full information at https://www.ftc.gov/legal-library/browse/cases-proceedings/122-3090-trendnet-inc-matter.

XI. Workplace Privacy

A. Government Employees.....590
O'Connor v. Ortega, 480 U.S. 709 (1987) 590

B. Employees and the privacy torts.....599
Clark v. Teamsters Local Union 651, 349 F.Supp.3d 605 (E.D. Ky. 2018) 599
Horgan v. Simmons, 704 F.Supp.2d 814 (N.D. Ill. 2010) 601

C. Laws on specific subjects.....604
1) Employees and the Electronic Communications Privacy Act (ECPA) 604
Owen v. Cigna, 188 F.Supp.3d 790 (N.D. Ill. 2016) 604
Sullinger v. Sullinger, 849 Fed.Appx. 513 (6th Cir. 2021) (unpublished) 606
Democracy Partners v. Project Veritas Action Fund, 285 F.Supp.3d 109 (D.D.C. 2018) 608
2) Cameras in the workplace 611
3) GPS monitoring of vehicles 612
Cunningham v. New York State Department of Labor, 997 N.E.2d 468 (N.Y. 2013) 613
4) Drug testing 616

Companies sometimes gather ambitious amounts of data on their employees. They do this to boost productivity, monitor compliance with workplace policies (consider data breach from Chapter 10), and prevent theft. In general, this is permissible. In a traditional employment situation, the employer controls the venue at which the work occurs, the tools that the employee uses, and the employee's basic comings and goings. It would seem strange if an employer could not, therefore, supervise its own facilities, its own tools, and the comings and goings of people who have voluntarily undertaken to work for them.

Despite this strong intuition in favor of allowing some, or even much, workplace surveillance, there is also a strong intuition that employees do not check all their privacy rights at the workplace door. Some issues are not practically or morally the employer's business. This is where privacy law runs squarely into antidiscrimination law. When asked what an employee should be permitted to keep private from their employer, answers will often include references to employee health, family planning, and religious beliefs. Federal law has much to say about discrimination based on any of those characteristics.[227]

This chapter is not intended to give the reader insight into antidiscrimination law. That is a complex and worthy topic best left to another book. Instead this chapter moves in another direction. What and when is an employer not permitted to monitor? And, if an employer wants to monitor this or that, what rules or regulations govern their ability to do so?

This chapter will proceed in three sections. First it examines how the Fourth Amendment controls government searches of government employees. Second, it considers state tort intrusion upon seclusion claims in the context of private employees. Despite their technical differences, the Fourth Amendment analysis and the tort analysis will ultimately turn on reasonableness determinations, meaning these completely different bodies of law will generally yield similar results. The chapter then closes by considering four different kinds of common

[227] One small piece of antidiscrimination law that will be relevant later: your employer is generally permitted to *ask* about all sorts of topics. They are not allowed to treat you differently based on the answers on certain topics, however. So it is not illegal to ask you your religion during a job interview. It is, however, 1) weird and 2) likely to give the applicant and a later court the sense that the answer *is* relevant to the hiring decision, which would be illegal.

monitoring: audio recording, video surveillance, GPS tracking, and drug testing. These four areas still feature the Fourth Amendment and tort claims discussed in Parts A and B, but also add some specific statutory regulations.

A. Government Employees

All government information collection is governed by the Fourth Amendment. As reviewed in Chapter 3, however, the protections of the Fourth Amendment work differently outside the law enforcement context. The below case is one of the pillars of the special needs doctrine, which was reviewed at length in Chapter 3.C.

Note that this opinion adds to the confusion and ambiguity in this area of law by having a plurality rather than majority as its lead opinion. Subsequent circuit cases tend to treat O'Connor's opinion as decisive, however.

O'Connor v. Ortega, 480 U.S. 709 (1987)

Justice O'CONNOR announced the judgment of the Court and delivered an opinion in which THE CHIEF JUSTICE, Justice WHITE, and Justice POWELL join.

This suit under 42 U.S.C. § 1983 presents two issues concerning the Fourth Amendment rights of public employees. First, we must determine whether the respondent, a public employee, had a reasonable expectation of privacy in his office, desk, and file cabinets at his place of work. Second, we must address the appropriate Fourth Amendment standard for a search conducted by a public employer in areas in which a public employee is found to have a reasonable expectation of privacy.

I

Dr. Magno Ortega, a physician and psychiatrist, held the position of Chief of Professional Education at Napa State Hospital (Hospital) for 17 years, until his dismissal from that position in 1981. As Chief of Professional Education, Dr. Ortega had primary responsibility for training young physicians in psychiatric residency programs.

In July 1981, Hospital officials, including Dr. Dennis O'Connor, the Executive Director of the Hospital, became concerned about possible improprieties in Dr. Ortega's management of the residency program. In particular, the Hospital officials were concerned with Dr. Ortega's acquisition of an Apple II computer for use in the residency program. The officials thought that Dr. Ortega may have misled Dr. O'Connor into believing that the computer had been donated, when in fact the computer had b'en financed by the possibly coerced contributions of residents. Additionally, the Hospital officials were concerned with charges that Dr. Ortega had sexually harassed two female Hospital employees, and had taken inappropriate disciplinary action against a resident.

On July 30, 1981, Dr. O'Connor requested that Dr. Ortega take paid administrative leave during an investigation of these charges. At Dr. Ortega's request, Dr. O'Connor agreed to allow Dr. Ortega to take two weeks' vacation instead of administrative leave. Dr. Ortega, however, was requested to stay off Hospital grounds for the duration of the investigation. On August 14, 1981, Dr. O'Connor informed Dr. Ortega that the investigation had not yet been completed, and that he was being placed on paid administrative leave. Dr. Ortega remained on administrative leave until the Hospital terminated his employment on September 22, 1981.

Dr. O'Connor selected several Hospital personnel to conduct the investigation, including an accountant, a physician, and a Hospital security officer. Richard Friday, the Hospital Administrator, led this "investigative team." At some point during the investigation, Mr. Friday made the decision to enter Dr. Ortega's office. The specific reason for the entry into Dr. Ortega's

office is unclear from the record. The petitioners claim that the search was conducted to secure state property. Initially, petitioners contended that such a search was pursuant to a Hospital policy of conducting a routine inventory of state property in the office of a terminated employee. At the time of the search, however, the Hospital had not yet terminated Dr. Ortega's employment; Dr. Ortega was still on administrative leave. Apparently, there was no policy of inventorying the offices of those on administrative leave. Before the search had been initiated, however, petitioners had become aware that Dr. Ortega had taken the computer to his home. Dr. Ortega contends that the purpose of the search was to secure evidence for use against him in administrative disciplinary proceedings.

The resulting search of Dr. Ortega's office was quite thorough. The investigators entered the office a number of times and seized several items from Dr. Ortega's desk and file cabinets, including a Valentine's Day card, a photograph, and a book of poetry all sent to Dr. Ortega by a former resident physician. These items were later used in a proceeding before a hearing officer of the California State Personnel Board to impeach the credibility of the former resident, who testified on Dr. Ortega's behalf. The investigators also seized billing documentation of one of Dr. Ortega's private patients under the California Medicaid program. The investigators did not otherwise separate Dr. Ortega's property from state property because, as one investigator testified, "[t]rying to sort State from non-State, it was too much to do, so I gave it up and boxed it up." Thus, no formal inventory of the property in the office was ever made. Instead, all the papers in Dr. Ortega's office were merely placed in boxes, and put in storage for Dr. Ortega to retrieve.

Dr. Ortega commenced this action against petitioners in Federal District Court under 42 U.S.C. § 1983, alleging that the search of his office violated the Fourth Amendment.

II

The strictures of the Fourth Amendment, applied to the States through the Fourteenth Amendment, have been applied to the conduct of governmental officials in various civil activities. Thus, we have held in the past that the Fourth Amendment governs the conduct of school officials, building inspectors, and Occupational Safety and Health Act inspectors. As we observed in *New Jersey v. T.L.O.* (1985), "[b]ecause the individual's interest in privacy and personal security 'suffers whether the government's motivation is to investigate violations of criminal laws or breaches of other statutory or regulatory standards,' . . . it would be 'anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior.'" Searches and seizures by government employers or supervisors of the private property of their employees, therefore, are subject to the restraints of the Fourth Amendment.

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ." Our cases establish that Dr. Ortega's Fourth Amendment rights are implicated only if the conduct of the Hospital officials at issue in this case infringed "an expectation of privacy that society is prepared to consider reasonable."

Because the reasonableness of an expectation of privacy, as well as the appropriate standard for a search, is understood to differ according to context, it is essential first to delineate the boundaries of the workplace context. The workplace includes those areas and items that are related to work and are generally within the employer's control. At a hospital, for example, the hallways, cafeteria, offices, desks, and file cabinets, among other areas, are all part of the workplace. These areas remain part of the workplace context even if the employee has placed personal items in them, such as a photograph placed in a desk or a letter posted on an employee bulletin board.

Not everything that passes through the confines of the business address can be considered part of the workplace context, however. An employee may bring closed luggage to the office prior to leaving on a trip, or a handbag or briefcase each workday. While whatever expectation of privacy the employee has in the existence and the outward appearance of the luggage is affected by its presence in the workplace, the employee's expectation of privacy in the *contents* of the luggage is not affected in the same way. The appropriate standard for a workplace search does not necessarily apply to a piece of closed personal luggage, a handbag or a briefcase that happens to be within the employer's business address.

Within the workplace context, this Court has recognized that employees may have a reasonable expectation of privacy against intrusions by police. As with the expectation of privacy in one's home, such an expectation in one's place of work is "based upon societal expectations that have deep roots in the history of the Amendment." Thus, in *Mancusi v. DeForte* (1968), the Court held that a union employee who shared an office with other union employees had a privacy interest in the office sufficient to challenge successfully the warrantless search of that office.

Given the societal expectations of privacy in one's place of work expressed in both *Oliver v. United States* (1984) and *Mancusi,* we reject the contention . . . that public employees can never have a reasonable expectation of privacy in their place of work. Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer. The operational realities of the workplace, however, may make *some* employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation. Indeed, in *Mancusi* itself, the Court suggested that the union employee did not have a reasonable expectation of privacy against his union supervisors. The employee's expectation of privacy must be assessed in the context of the employment relation. An office is seldom a private enclave free from entry by supervisors, other employees, and business and personal invitees. Instead, in many cases offices are continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits. Simply put, it is the nature of government offices that others—such as fellow employees, supervisors, consensual visitors, and the general public—may have frequent access to an individual's office. We agree with Justice SCALIA that "[c]onstitutional protection against *unreasonable* searches by the government does not disappear merely because the government has the right to make reasonable intrusions in its capacity as employer," but some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable. Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.

The Court of Appeals concluded that Dr. Ortega had a reasonable expectation of privacy in his office, and five Members of this Court agree with that determination. Because the record does not reveal the extent to which Hospital officials may have had work-related reasons to enter Dr. Ortega's office, we think the Court of Appeals should have remanded the matter to the District Court for its further determination. But regardless of any legitimate right of access the Hospital staff may have had to the office as such, we recognize that the undisputed evidence suggests that Dr. Ortega had a reasonable expectation of privacy in his desk and file cabinets. Dr. Ortega did not share his desk or file cabinets with any other employees. Dr. Ortega had occupied the office for 17 years and he kept materials in his office, which included personal correspondence, medical files, correspondence from private patients unconnected to the Hospital, personal financial records, teaching aids and notes, and personal gifts and mementos. The files on physicians in residency training were kept outside Dr. Ortega's office. Indeed, the only items found by the investigators were apparently personal items because, with the

exception of the items seized for use in the administrative hearings, all the papers and effects found in the office were simply placed in boxes and made available to Dr. Ortega. Finally, we note that there was no evidence that the Hospital had established any reasonable regulation or policy discouraging employees such as Dr. Ortega from storing personal papers and effects in their desks or file cabinets, although the absence of such a policy does not create an expectation of privacy where it would not otherwise exist.

On the basis of this undisputed evidence, we accept the conclusion of the Court of Appeals that Dr. Ortega had a reasonable expectation of privacy at least in his desk and file cabinets.

III

Having determined that Dr. Ortega had a reasonable expectation of privacy in his office, the Court of Appeals simply concluded without discussion that the "search . . . was not a reasonable search under the [F]ourth [A]mendment." But as we have stated in *T.L.O.,* "[t]o hold that the Fourth Amendment applies to searches conducted by [public employers] is only to begin the inquiry into the standards governing such searches . . . . [W]hat is reasonable depends on the context within which a search takes place." Thus, we must determine the appropriate standard of reasonableness applicable to the search. A determination of the standard of reasonableness applicable to a particular class of searches requires "balanc[ing] the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." In the case of searches conducted by a public employer, we must balance the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace.

"[I]t is settled . . . that 'except in certain carefully defined classes of cases, a search of private property without proper consent is "unreasonable" unless it has been authorized by a valid search warrant.'" There are some circumstances, however, in which we have recognized that a warrant requirement is unsuitable. In particular, a warrant requirement is not appropriate when "the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search." Or, as Justice BLACKMUN stated in *T.L.O.,* "[o]nly in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." In *Marshall v. Barlow's, Inc.* (1978), for example, the Court explored the burdens a warrant requirement would impose on the Occupational Safety and Health Act regulatory scheme, and held that the warrant requirement was appropriate only after concluding that warrants would not "impose serious burdens on the inspection system or the courts, [would not] prevent inspections necessary to enforce the statute, or [would not] make them less effective." In *New Jersey v. T.L.O.,* we concluded that the warrant requirement was not suitable to the school environment, because such a requirement would unduly interfere with the maintenance of the swift and informal disciplinary procedures needed in the schools.

There is surprisingly little case law on the appropriate Fourth Amendment standard of reasonableness for a public employer's work-related search of its employee's offices, desks, or file cabinets. Generally, however, the lower courts have held that any "work-related" search by an employer satisfies the Fourth Amendment reasonableness requirement. Others have suggested the use of a standard other than probable cause. The only cases to imply that a warrant should be required involve searches that are not work related or searches for evidence of criminal misconduct.

The legitimate privacy interests of public employees in the private objects they bring to the workplace may be substantial. Against these privacy interests, however, must be balanced the realities of the workplace, which strongly suggest that a warrant requirement would be

unworkable. While police, and even administrative enforcement personnel, conduct searches for the primary purpose of obtaining evidence for use in criminal or other enforcement proceedings, employers most frequently need to enter the offices and desks of their employees for legitimate work-related reasons wholly unrelated to illegal conduct. Employers and supervisors are focused primarily on the need to complete the government agency's work in a prompt and efficient manner. An employer may have need for correspondence, or a file or report available only in an employee's office while the employee is away from the office. Or, as is alleged to have been the case here, employers may need to safeguard or identify state property or records in an office in connection with a pending investigation into suspected employee misfeasance.

In our view, requiring an employer to obtain a warrant whenever the employer wished to enter an employee's office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unduly burdensome. Imposing unwieldy warrant procedures in such cases upon supervisors, who would otherwise have no reason to be familiar with such procedures, is simply unreasonable. In contrast to other circumstances in which we have required warrants, supervisors in offices such as at the Hospital are hardly in the business of investigating the violation of criminal laws. Rather, work-related searches are merely incident to the primary business of the agency.

Whether probable cause is an inappropriate standard for public employer searches of their employees' offices presents a more difficult issue. For the most part, we have required that a search be based upon probable cause, but as we noted in *New Jersey v. T.L.O.,* "[t]he fundamental command of the Fourth Amendment is that searches and seizures be reasonable, and although 'both the concept of probable cause and the requirement of a warrant bear on the reasonableness of a search, . . . in certain limited circumstances neither is required.'" Thus, "[w]here a careful balancing of governmental and private interests suggests that the public interest is best served by a Fourth Amendment standard of reasonableness that stops short of probable cause, we have not hesitated to adopt such a standard." We have concluded, for example, that the appropriate standard for administrative searches is not probable cause in its traditional meaning. Instead, an administrative warrant can be obtained if there is a showing that reasonable legislative or administrative standards for conducting an inspection are satisfied.

The governmental interest justifying work-related intrusions by public employers is the efficient and proper operation of the workplace. Government agencies provide myriad services to the public, and the work of these agencies would suffer if employers were required to have probable cause before they entered an employee's desk for the purpose of finding a file or piece of office correspondence. Indeed, it is difficult to give the concept of probable cause, rooted as it is in the criminal investigatory context, much meaning when the purpose of a search is to retrieve a file for work-related reasons. Similarly, the concept of probable cause has little meaning for a routine inventory conducted by public employers for the purpose of securing state property. To ensure the efficient and proper operation of the agency, therefore, public employers must be given wide latitude to enter employee offices for work-related, noninvestigatory reasons.

We come to a similar conclusion for searches conducted pursuant to an investigation of work-related employee misconduct. Even when employers conduct an investigation, they have an interest substantially different from "the normal need for law enforcement." In our view, therefore, a probable cause requirement for searches of the type at issue here would impose intolerable burdens on public employers. The delay in correcting the employee misconduct caused by the need for probable cause rather than reasonable suspicion will be translated into tangible and often irreparable damage to the agency's work, and ultimately to the public interest. Additionally, while law enforcement officials are expected to "schoo[l] themselves in the niceties of probable cause," no such expectation is generally applicable to public employers,

at least when the search is not used to gather evidence of a criminal offense. It is simply unrealistic to expect supervisors in most government agencies to learn the subtleties of the probable cause standard.

Balanced against the substantial government interests in the efficient and proper operation of the workplace are the privacy interests of government employees in their place of work which, while not insubstantial, are far less than those found at home or in some other contexts. As with the building inspections in *Camara v. Municipal Court* (1967), the employer intrusions at issue here "involve a relatively limited invasion" of employee privacy. Government offices are provided to employees for the sole purpose of facilitating the work of an agency. The employee may avoid exposing personal belongings at work by simply leaving them at home.

In sum, we conclude that the "special needs, beyond the normal need for law enforcement make the . . . probable-cause requirement impracticable" for legitimate work-related, noninvestigatory intrusions as well as investigations of work-related misconduct. A standard of reasonableness will neither unduly burden the efforts of government employers to ensure the efficient and proper operation of the workplace, nor authorize arbitrary intrusions upon the privacy of public employees. We hold, therefore, that public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this reasonableness standard, both the inception and the scope of the intrusion must be reasonable.

Ordinarily, a search of an employee's office by a supervisor will be "justified at its inception" when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file. Because petitioners had an "individualized suspicion" of misconduct by Dr. Ortega, we need not decide whether individualized suspicion is an essential element of the standard of reasonableness that we adopt today. The search will be permissible in its scope when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct]."

IV

We believe that both the District Court and the Court of Appeals were in error because summary judgment was inappropriate. The parties were in dispute about the actual justification for the search, and the record was inadequate for a determination on motion for summary judgment of the reasonableness of the search and seizure.

On remand, therefore, the District Court must determine the justification for the search and seizure, and evaluate the reasonableness of both the inception of the search and its scope.

Justice SCALIA, concurring in the judgment.

The plurality opinion instructs the lower courts that existence of Fourth Amendment protection for a public employee's business office is to be assessed "on a case-by-case basis," in light of whether the office is "so open to fellow employees or the public that no expectation of privacy is reasonable." No clue is provided as to how open "so open" must be; much less is it suggested how police officers are to gather the facts necessary for this refined inquiry. Even if I did not disagree with the plurality as to what result the proper legal standard should produce in the case before us, I would object to the formulation of a standard so devoid of content that it produces rather than eliminates uncertainty in this field.

I cannot agree, moreover, with the plurality's view that the reasonableness of the expectation of privacy (and thus the existence of Fourth Amendment protection) changes "when an intrusion is by a supervisor rather than a law enforcement official." The identity of the

searcher (police v. employer) is relevant not to whether Fourth Amendment protections apply, but only to whether the search of a protected area is reasonable. Pursuant to traditional analysis the former question must be answered on a more "global" basis. Where, for example, a fireman enters a private dwelling in response to an alarm, we do not ask whether the occupant has a reasonable expectation of privacy (and hence Fourth Amendment protection) vis-à-vis firemen, but rather whether—given the fact that the Fourth Amendment covers private dwellings—intrusion for the purpose of extinguishing a fire is reasonable. A similar analysis is appropriate here.

I would hold, therefore, that the offices of government employees, and *a fortiori* the drawers and files within those offices, are covered by Fourth Amendment protections as a general matter. (The qualifier is necessary to cover such unusual situations as that in which the office is subject to unrestricted public access, so that it is "expose[d] to the public" and therefore "not a subject of Fourth Amendment protection.") Since it is unquestioned that the office here was assigned to Dr. Ortega, and since no special circumstances are suggested that would call for an exception to the ordinary rule, I would agree with the District Court and the Court of Appeals that Fourth Amendment protections applied.

The case turns, therefore, on whether the Fourth Amendment was violated—*i.e.,* whether the governmental intrusion was reasonable. It is here that the government's status as employer, and the employment-related character of the search, become relevant. While as a general rule warrantless searches are *per se* unreasonable, we have recognized exceptions when "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable . . . ." *New Jersey v. T.L.O.* (BLACKMUN, J., concurring in judgement). Such "special needs" are present in the context of government employment. The government, like any other employer, needs frequent and convenient access to its desks, offices, and file cabinets for work-related purposes. I would hold that government searches to retrieve work-related materials or to investigate violations of workplace rules—searches of the sort that are regarded as reasonable and normal in the private-employer context—do not violate the Fourth Amendment. Because the conflicting and incomplete evidence in the present case could not conceivably support summary judgment that the search did not have such a validating purpose, I agree with the plurality that the decision must be reversed and remanded.

Justice BLACKMUN, with whom Justice BRENNAN, Justice MARSHALL, and Justice STEVENS join, dissenting.

The facts of this case are simple and straightforward. Dr. Ortega had an expectation of privacy in his office, desk, and file cabinets, which were the target of a search by petitioners that can be characterized only as investigatory in nature. Because there was no "special need" to dispense with the warrant and probable-cause requirements of the Fourth Amendment, I would evaluate the search by applying this traditional standard. Under that standard, this search clearly violated Dr. Ortega's Fourth Amendment rights.

Moreover, as the plurality appears to recognize, the precise extent of an employee's expectation of privacy often turns on the nature of the search. This observation is in accordance with the principle that the Fourth Amendment may protect an individual's expectation of privacy in one context, even though this expectation may be unreasonable in another. Thus, although an employee might well have no reasonable expectation of privacy with respect to an occasional visit by a fellow employee, he would have such an expectation as to an afterhours search of his locked office by an investigative team seeking materials to be used against him at a termination proceeding.

Finally and most importantly, the reality of work in modern time, whether done by public or private employees, reveals why a public employee's expectation of privacy in the workplace should be carefully safeguarded and not lightly set aside. It is, unfortunately, all too true that the workplace has become another home for most working Americans. Many

employees spend the better part of their days and much of their evenings at work. Consequently, an employee's private life must intersect with the workplace, for example, when the employee takes advantage of work or lunch breaks to make personal telephone calls, to attend to personal business, or to receive personal visitors in the office. As a result, the tidy distinctions (to which the plurality alludes) between the workplace and professional affairs, on the one hand, and personal possessions and private activities, on the other, do not exist in reality. Not all of an employee's private possessions will stay in his or her briefcase or handbag. Thus, the plurality's remark that the "employee may avoid exposing personal belongings at work by simply leaving them at home," reveals on the part of the Members of the plurality a certain insensitivity to the "operational realities of the workplace" they so value.

At the outset of its analysis, the plurality observes that an appropriate standard of reasonableness to be applied to a public employer's search of the employee's workplace is arrived at from "balancing" the privacy interests of the employee against the public employer's interests justifying the intrusion. Under traditional Fourth Amendment jurisprudence, however, courts abandon the warrant and probable-cause requirements, which constitute the standard of reasonableness for a government search that the Framers established, "[o]nly in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable . . . ." In sum, only when the practical realities of a particular situation suggest that a government official cannot obtain a warrant based upon probable cause without sacrificing the ultimate goals to which a search would contribute, does the Court turn to a "balancing" test to formulate a standard of reasonableness for this context.

In *New Jersey v. T.L.O.*, I faulted the Court for neglecting this "crucial step" in Fourth Amendment analysis. The plurality repeats here the *T.L.O.* Court's error in analysis. Although the plurality mentions the "special need" step, it turns immediately to a balancing test to formulate its standard of reasonableness. This error is significant because, given the facts of this case, no "special need" exists here to justify dispensing with the warrant and probable-cause requirements. As observed above, the facts suggest that this was an investigatory search undertaken to obtain evidence of charges of mismanagement at a time when Dr. Ortega was on administrative leave and not permitted to enter the Hospital's grounds. There was no special practical need that might have justified dispensing with the warrant and probable-cause requirements. Without sacrificing their ultimate goal of maintaining an effective institution devoted to training and healing, to which the disciplining of Hospital employees contributed, petitioners could have taken any evidence of Dr. Ortega's alleged improprieties to a magistrate in order to obtain a warrant.

Furthermore, this seems to be exactly the kind of situation where a neutral magistrate's involvement would have been helpful in curtailing the infringement upon Dr. Ortega's privacy. Petitioners would have been forced to articulate their exact reasons for the search and to specify the items in Dr. Ortega's office they sought, which would have prevented the general rummaging through the doctor's office, desk, and file cabinets. Thus, because no "special need" in this case demanded that the traditional warrant and probable-cause requirements be dispensed with, petitioners' failure to conduct the search in accordance with the traditional standard of reasonableness should end the analysis, and the judgment of the Court of Appeals should be affirmed.

Notes

1. More than ten years after this opinion, and about sixteen years after the search, the Ninth Circuit upheld a jury award in favor of Dr. Ortega. In holding that the hospital did not have a defense under qualified immunity, the court focused on four key facts:

> (1) that the defendants, under the pretense of conducting an "inventory" of state property in order to separate personal from official materials, conducted instead a purely indiscriminate fishing expedition through his most personal belongings in hopes of discovering some evidence that might be useful at an adversary administrative hearing;
>
> (2) that the repeated intrusions and examinations of Dr. Ortega's private possessions, including his purely personal belongings, clearly exceeded the scope of a reasonable work-related search;
>
> (3) that the defendants retained *all* of the property that had been in his office, both personal and official, in one undivided mass; and
>
> (4) that when their first explanation was exposed as false, the defendants then offered other equally untruthful rationales for their conduct.

Ortega v. O'Connor, 146 F.3d 1149, 1159 (9th Cir. 1998). Notably, the court disregarded sexual harassment concerns as a justification for the search, consistent with pretrial rulings. Were an employer legitimately concerned that a public hospital doctor or public university professor was engaged in sexual harassment, would that justify a search of personal possessions housed in their office?

2. How well do the dissent's intuitions about use of the workplace match your personal experience? Much has changed about the structure of the American economy between the 1980s and the present. Was your last office full of personal effects? What about your last workplace computer? As will be seen below, many recent cases are about electronic files rather than filing cabinets.
3. O'Connor's opinion turns the fundamental question for employee searches into one of reasonableness. This presents something of a challenge, as it is difficult to predict what a judge might consider reasonable. It also allows for a neat mapping of the Fourth Amendment test onto the tort of intrusion upon seclusion, however. The Fourth Amendment test asks 1) whether there is a reasonable expectation of privacy and 2) whether a violation of that expectation is constitutionally reasonable. The intrusion upon seclusion tort asks 1) whether there is a violation of privacy and 2) whether that violation is highly offensive to a reasonable person. For example, consider the private employer case of *Hernandez v. Hillsides, Inc.*, 47 Cal.4th 272 (Cal. 2009). There the employer—a private residential facility for neglected and abused children—installed a camera in the office assigned to the two plaintiff employees. The court readily concluded that this violated the privacy element of the tort—it was the plaintiffs' private office in roughly the same way as Dr. Ortega's office. But the employer only used the camera after hours, with the intent of catching a third party who was using the office to view pornography. The plaintiffs themselves never appeared in any of the resultant video. In the words of the court: "Given the apparent risks under existing law of doing nothing to avert the problem, and the limited range of available solutions, defendants' conduct was not highly offensive for purposes of establishing a tortious intrusion into private matters." That sounds much like holding that a Fourth Amendment search was reasonable.
4. Courts often comment on efforts to limit the scope of government workplace investigations. For example, when the Supreme Court approved the warrantless investigation of a police officer's pager messages, it noted that the investigator had redacted the contents of any message that the officer sent while off-duty. *City of Ontario, California v. Quon*, 560 U.S. 746, 762 (2010).

B. Employees and the privacy torts

Employees almost always have the option of bringing an intrusion upon seclusion action. This tort technically works the same way in the employment context as it does elsewhere, but there are two important practical differences. First, the need for employers to regulate their workplaces often makes intrusions not highly offensive. Employers have better reasons than neighbors to get into your business. Second, employers control the physical, digital, and social spaces in which employees work. Since expectations of privacy are highly contextual, this gives employers a lot of control. A clever employer can often make sure that employees only have the privacy expectations that employers want them to have.

Clark v. Teamsters Local Union 651, 349 F.Supp.3d 605 (E.D. Ky. 2018)

Danny C. Reeves, United States District Judge

Plaintiffs Sara Clark and Carol Estepp filed this action against Teamsters Local Union 651 ("Local 651"), Michael Philbeck, and International Brotherhood of Teamsters ("IBT") in June 2017. Clark and Estepp are former employees of Teamsters Local Union 651. The plaintiffs were originally salaried employees, but were switched to an hourly rate in August 2016. The plaintiffs allege they would clock out and continue to work or deliver packages on their way home.

The plaintiffs claim that Philbeck used derogatory language against women and commented on their appearances throughout their time at Local 651. Estepp testified that Philbeck would kiss her on the cheek every morning, asked her to sit on his lap, and called her "mom." The plaintiffs also allege that Philbeck used profanities when they disregarded his orders. Further, the plaintiffs contend that they were fearful that Philbeck would harm or take personnel action against them.

Clark testified that the situation escalated in June 2016. While Estepp looked on, Philbeck cursed at Clark and told her to leave Local 651 after she refused his request to modify his 401(k) contributions in an effort to hide money from his wife, whom he was divorcing. Following this exchange, Clark sent a letter in June 2016 to the Local 651 Executive Board describing verbal abuse and a hostile environment at Local 651. [Following this is an extended discussion of the toxic office politics involving Clark and Philbeck. The only relevant facts are that Clark does not appear to have engaged in misconduct and that Clark is eventually terminated.]

Following Clark's termination, Local 651's administrative assistant Stephanie Buchenroth used a lost password function and changed the passwords on Clark's Local 651 e-mail and Dropbox accounts. Clark created the Dropbox account using her work e-mail. Buchenroth subsequently searched the Dropbox and e-mail. The Dropbox account contained both work-related and personal documents. The Dropbox was accessed while IBT was on site at Local 651 performing an audit.

Invasion of Privacy Claim

Administrative assistant Stephanie Buchenroth accessed Clark's computer after her termination and used a lost password function to recover and review the files in Clark's Dropbox to search for work-related files. While Clark contends that the Dropbox was her personal account, the account was linked to her Teamsters e-mail address to which she lost access when terminated. Clark believes that Buchenroth "hacked" into her Dropbox account by using the lost password function. Local 651, however, takes the position that it "had the right to

discontinue Clark's access to that e-mail account at any time, which includes Local's 651's right and ability to change Clark's e-mail password."

Under the facts presented, Clark cannot prevail on theories that Buchenroth's actions constitute an intrusion upon her seclusion and unlawful access to her computer in violation of Kentucky statutes. This Court has previously relied on the definition of intrusion upon seclusion . . . which is "intentional intrusion, physical or otherwise, upon the solitude or seclusion of another . . . if the intrusion would be highly offensive to a reasonable person." To prevail, a plaintiff must demonstrate "(1) an intentional intrusion by the defendant, (2) into a matter the plaintiff has a right to keep private, and (3) which is highly offensive to a reasonable person." "What constitutes a private matter is dependent upon whether the plaintiff has a reasonable expectation of privacy in the subject information." Potential intrusions include "investigation or examination into [her] private concerns, as by opening [her] private and personal mail, searching [her] safe or wallet, [or] examining [her] private bank account." Restatement (Second) of Torts § 652B, cmt. B (1977).

While not explicitly addressed by the Sixth Circuit, district courts have held that an employee does not have a reasonable expectation of privacy in e-mails sent or received using a work e-mail address. *See Garrity v. John Hancock Mut. Life Ins. Co.* (D. Mass. 2002) (explaining even in the absence of a company e-mail policy, employees did not have a reasonable expectation of privacy in their work e-mail); *Smyth v. Pillsbury Co.* (E.D. Pa. 1996) (holding no reasonable expectation of privacy in voluntary e-mail communications made by an employee, notwithstanding any assurance that e-mails would not be intercepted by management). If individuals do not have a reasonable expectation of privacy in their work e-mails, then it logically follows that individuals do not have a reasonable expectation of privacy in a Dropbox account that is tied to their work e-mail and that they lose access to if they lose access to the e-mail.

In *Garrity*, the plaintiffs admitted that they knew the defendant employer had the ability to access e-mails over the company's intranet system. However, they argued that their e-mails were private because they were password protected and stored in personal folders. The court rejected this argument, concluding that the plaintiffs had no reasonable expectation of privacy in their work e-mails. It further explained that, even if the plaintiffs had a reasonable expectation of privacy in their work e-mails, the defendant had a legitimate business interest in monitoring the e-mails to keep the workplace free of harassment.

For the same reasons, Clark does not have a reasonable expectation of privacy in the Dropbox account, which stored a mixture of work-related and personal documents and was tied to her work e-mail. Further, even if she did have such an expectation, Local 651 had a legitimate business purpose to recover documents related to Local 651's operations from Clark's e-mail and Dropbox account.

The plaintiff also argues that, by accessing her Dropbox account, the defendants unlawfully accessed her computer. Clark relies on Kentucky's negligence *per se* statute and the state statute pertaining to the unlawful access to a computer. Ky. Rev. Stat. §§ 434.845-.853; 446.070. To establish unlawful access, a plaintiff must establish that "a person . . . without the effective consent of the owner, knowingly and willfully, directly or indirectly accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof[.]"But, as previously explained, Clark does not have a reasonable expectation of privacy in the Dropbox account, and there is no violation of the statute.

There is no genuine dispute of material fact with respect to Clark's invasion of privacy claim and Local 651 and Philbeck are entitled to summary judgment on Count IV and Count V.

Notes

1. Perhaps unsurprisingly, this case also involved claims of workplace harassment, defamation, and violations of labor law. The plaintiffs are only allowed to proceed with one of their main defamation theories and their claims for uncompensated overtime pay.
2. A parallel case involving a government employer reached a mostly-similar result. In *Bowers v. County of Taylor*, 598 F.Supp.3d 719 (W.D. Wis. 2022), the court held that it was a Fourth Amendment search to access an employee's personal Dropbox account even though it was linked to the employee's work email, but that the defendants were entitled to qualified immunity given that the law did not previously clearly establish this. The court also would have held the search to be reasonable given that there was cause to expect to find evidence of work-related misconduct.
3. Employee work email accounts are not private from employers. Employee Dropbox accounts linked to work emails are not private from employers. Are employee Dropbox accounts linked to personal emails private from employers if the account automatically syncs files to the work computers? Imagine a person is fired. IT goes to examine their computer and finds that the ex-employee's personal Dropbox has synced files to the hard drive. What should they be allowed to do at that point?

Horgan v. Simmons, 704 F.Supp.2d 814 (N.D. Ill. 2010)

RUBEN CASTILLO, District Judge.

Kenneth Horgan brings this action alleging employment discrimination and invasion of privacy against Timothy Simmons and Morgan Services. Plaintiff claims that Defendants unlawfully terminated him because of his disability and impermissibly inquired as to his disability under the Americans with Disabilities Act (ADA). In addition, Plaintiff claims that Defendants invaded his privacy under Illinois state law.

Plaintiff has been diagnosed as HIV positive for the past ten years, but kept his status confidential, disclosing his medical condition only to his close friends. In February 2001, he began working for Morgan, a linen and uniform rental services company, as a sales manager in Los Angeles. In January 2008, Defendants promoted him to General Manager of the Chicago facility. Plaintiff claims that his HIV positive status never interfered with his ability to perform the essential functions of his job and that he "has always met or exceeded Morgan's legitimate expectations."

Simmons is Morgan's president and was Plaintiff's supervisor in Chicago. On July 15, 2009, Plaintiff alleges that Simmons asked to meet with him for what Simmons termed a "social visit." During their visit, Plaintiff alleges that Simmons "told plaintiff that he was really worried about him." When Plaintiff responded by discussing his work performance, Plaintiff claims that Simmons cut him off saying "this is not about results." Plaintiff alleges that Simmons then "demanded" to know what was going on with him, telling Plaintiff that "if there was something medical going on, [he] needed to know." Plaintiff insisted that there was nothing that affected his ability to work. However, Plaintiff claims that Simmons "continued to insist there was something physical or mental that was affecting [Plaintiff]." Plaintiff claims he was "compelled to tell Simmons that he was HIV positive," but he assured Simmons that his status did not affect his ability to do his job.

Plaintiff alleges that Simmons then asked him about his prognosis. Plaintiff responded that "he had been HIV positive for a long time and that the condition was under control and that his T-cell count was over 300." Next, Plaintiff alleges that Simmons asked "what would happen if his T-cell count went below 200," and Plaintiff replied that he would then have AIDS. After urging Plaintiff to inform his family about his condition, Plaintiff alleges that Simmons asked him "how he could ever perform his job with his HIV positive condition and how he could

continue to work with a terminal illness." Additionally, Plaintiff claims that Simmons told him "that a General Manager needs to be respected by the employees and have the ability to lead," and indicated that he "did not know how [Plaintiff] could lead if the employees knew about his condition."

Simmons allegedly ended the meeting by telling Plaintiff that he needed "to recover" and that he should "go on vacation" and "leave the plant immediately." Simmons then told Plaintiff that he would discuss the situation with Morgan's owner. The next day, Plaintiff alleges that he received a copy of an email sent to all general managers and corporate staff indicating that "effective immediately" Plaintiff was "no longer a member of Morgan [ ]."

Count II—Impermissible Medical Inquiry

Plaintiff alleges that the questions posed by Simmons on July 15, 2009, "constituted prohibited inquires in violation of the ADA." The ADA prohibits "inquiries of an employee as to whether [an] employee is an individual with a disability or as to the nature or severity of the disability, unless such examination or inquiry is shown to be job-related and consistent with business necessity." 42 U.S.C. § 12112(d)(4). Here, Plaintiff alleges that Simmons demanded to know whether "something medical [was] going on" and "continued to insist there was something physical or mental that was affecting [Plaintiff]." Plaintiff claims that based on this questioning, he was "compelled to tell Simmons that he was HIV positive." Further, Simmons allegedly asked Plaintiff about his prognosis and what would happen if his T-cell count fell below 200. Such questioning constitutes an inquiry as to whether Plaintiff had a disability and the nature and severity of the disability, and is thus prohibited by the ADA.

Nevertheless, Defendants argue that after Plaintiff disclosed his HIV positive status, they were "entitled to ask questions about the stage to which the virus had progressed because it related to [Plaintiff's] possible fitness to work both presently and in the future," and that such questioning was "job-related and consistent with business necessity." Again, Plaintiff alleges that he was "compelled to tell Simmons that he was HIV positive," and disclosed this information only after an impermissible inquiry under the ADA. Further, Plaintiff's allegation that he repeatedly insisted that nothing (including his HIV status) affected his ability to perform his duties directly rebuts Defendants' assertion that the questioning was necessary to discern whether Plaintiff could "cope with the demands and responsibilities of his job."

Thus, Plaintiff has sufficiently pled a claim for an impermissible inquiry under the ADA and Defendants' motion to dismiss on this basis is denied.

Count III—State Law Claim

Plaintiff alleges that Defendants' invaded his privacy by intruding upon his seclusion in violation of Illinois law. Intrusion upon the seclusion of another is one of four torts based on an invasion of privacy. While the Illinois Supreme Court has not explicitly recognized the tort of intrusion upon the seclusion of another, all of the Illinois Appellate Courts have recognized such a tort.

To begin, Defendants claim that Plaintiff "disclosed his condition as HIV [positive], without objecting or otherwise invoking any claim to confidentiality." Plaintiff, however, argues that the complaint illustrates that "Simmons would not take no for an answer," and therefore "[i]t cannot be said that [he] authorized the disclosure of his medical condition." However, even if the disclosure of Plaintiff's HIV status was not voluntary, Defendants' questioning does not give rise to the level of intrusion actionable under the tort. *Compare Karraker v. Rent–A–Center, Inc.* (C.D. Ill. 2003) (finding that plaintiffs' allegations of employers inquiries about personal information including sexual preferences and orientation, religious beliefs and practices and medical conditions were insufficient for a claim of intrusion upon the seclusion of another under Illinois law), *and Kelly v. Mercoid Corp.* (N.D. Ill. 1991) (requiring an employee to submit to urinalysis testing does not constitute an unreasonable intrusion into the seclusion of another),

with Benitez v. KFC Nat'l Mgmt. Co. (Ill. App. 2d 1999) ("[e]xamples of actionable intrusion upon seclusion would include invading someone's home, illegally searching someone's shopping bag in a store, eavesdropping by wiretapping, peering into the windows of a private home, or making persistent and unwanted telephone calls"). Therefore, Simmons' questioning fails to establish a sufficient "prying" into a zone of solitude necessary to establish a claim under the tort. Accordingly, Defendants' motion to dismiss on this basis is granted.

Notes

1. This book does not purport to examine the Americans with Disabilities Act or any feature of disability law. Given how firmly the intrusion upon seclusion claim is rejected here, however, not including this portion of the ADA analysis might leave students with the impression that Simmons' alleged conduct was legal. It was not. But it was illegal because it implicated an antidiscrimination law. From a tort privacy perspective, these questions were not unduly intrusive.
2. One might have difficulty crafting a rule that would make Simmons' questions an intrusion upon seclusion. Imagine I am discussing the coming month with my faculty assistant and she mentions that she will be out a particular week. I ask why, and she feels compelled to say that she is celebrating a religious holiday. She has just revealed a personal fact. My idle inquiry is a far step from the hounding attributed to Simmons, but how best to formalize the distinction? And is the hostility of the defendant a necessary element here? What if Simmons had been nosey out of idle curiosity, or out of a genuine desire to help and accommodate the plaintiff? Would that be highly offensive?

Consider how employers can work to proactively prevent intrusion upon seclusion claims. *O'Connor v. Ortega* focused on how private a physical office was, how it contained a lot of highly personal possessions, and how it was generally not entered or examined by other staff. An employer could simply not allow employees that level of privacy. Some offices have glass doors. Some have policies about what kinds of personal possessions are allowed. Some have policies stating that personal possessions are subject to search. Consider the 2024 version of the Northwestern University Staff Handbook.[228]

> **Privacy.** Northwestern places a high value on privacy and recognizes its critical importance in an academic setting. However, given that the University information systems are provided for the purpose of conducting Northwestern business, the University maintains the right to access system accounts. Although Northwestern does not routinely monitor the content of communications or transmissions using University infrastructure, at times, legitimate reasons exist for persons other than the account holders to access these services.
>
> **Equipment and Facilities.** Northwestern equipment and facilities provided for use by staff—such as lockers, offices, office furniture, phones, mobile devices, tablets, and personal and network computers, their files, CDs, and peripherals—are Northwestern property and are fully accessible to the University at all times.

Imagine Northwestern wants to conduct a top-to-bottom search of a faculty assistant's office. If one takes this document seriously (and courts are likely to do so), that search could legally include desk drawers, filing cabinets, and anything else owned by the university. There is, however, nothing obvious in the handbook that would give Northwestern the right to search a staff member's backpack, even were it in the office. Were said backpack ticking, smoking, or smelling of a disruptive or illegal substance, however, it would likely not be highly offensive to search within.

---

[228] NORTHWESTERN OFFICE OF HUMAN RESOURCES, STAFF HANDBOOK (May 2024), https://hr.northwestern.edu/documents/nu_staff_handbook.pdf.

C. Laws on specific subjects

The privacy torts (here almost exclusively meaning intrusion upon seclusion) may provide little help to an employee unless their employer has foolishly allowed them to expect more privacy than the employer planned to give them. But there are still some ways that modern technology has allowed employers to violate the few privacy expectations that employees retain. Some of these ways are sufficiently egregious that they have prompted their own statutes, freeing employees from having to rely on basic tort claims.

1) Employees and the Electronic Communications Privacy Act (ECPA)

This is likely your second or third journey into the mysteries of the ECPA and its components: the Wiretap Act and the Stored Communications Act. As such, it will not be introduced at length. Please see Chapter 3.D to remind yourself of any points not explained in the below opinions.

Owen v. Cigna, 188 F.Supp.3d 790 (N.D. Ill. 2016)

JOHN Z. LEE, United States District Judge

Plaintiff Lois Owen claims that Defendants Paul Cigna, Professional Consultants, Inc., and Noah Edmeier violated multiple federal laws when they accessed her private email account through her former work computer. Defendants have moved under Fed. R. Civ. P. 12(b)(6) to dismiss . . . .

According to Owen's complaint, she worked for Cigna and Professional Consultants, Inc. (PCI) until July 2013. After leaving her job at PCI, Owen filed a complaint with the Illinois Human Rights Commission (IHRC), in which she accused her former employers of sexual harassment and of creating a hostile work environment.

During discovery in the IHRC case, Owen learned that "Defendants, including PCI's technology consultant Noah Edmeier, accessed her email account without her permission after she left work." She has attached to her complaint Cigna's affidavit from the IHRC case, where Cigna confirms that Defendants did indeed acquire Owen's personal emails through her former work computer, which was the property of PCI. Neither the complaint nor the accompanying exhibits indicate precisely how Defendants used her former work computer to access her personal emails, which Owen alleges were "stored on a server at att.net," rather than on the computer.

The emails in question, which Cigna attached to his affidavit, contained sexually explicit content, including photos of nude women (though not of Owen herself). Owen alleges that she has been "damaged in excess of $5,000.00 as a result of the access to her account, including publication of her confidential email correspondence."

I. Federal Wiretap Act, 18 U.S.C. §§ 2510–22

Defendants argue that Owen's Wiretap Act claim must be dismissed because her own allegations show that Defendants acquired her emails after she stopped working at PCI, rather than at the time the emails were sent. Because Defendants' acquisition of the emails was not "contemporaneous" with the emails being sent or received, Defendants argue that their acquisition does not qualify as an "interception" as required by the Wiretap Act.

The Court is persuaded that Defendants could only have violated the Wiretap Act if they accessed Owen's emails contemporaneously with the emails' transmission or receipt. The concept of interception suggests contemporaneousness, and, as the Third Circuit explained in *Fraser v. Nationwide Mutual Insurance Co.* (3d Cir. 2003), Congress has chosen not to overrule the cases that have read a contemporaneousness requirement into the Wiretap Act when the Act was amended.

The allegations in Owen's complaint, which must be credited at this stage, establish that Defendants did not access her emails contemporaneously with the emails' transmission or receipt. Owen alleges that Defendants accessed her emails after she stopped working for PCI in July 2013, and she has attached the emails to her complaint, the most recent of which was sent in May 2011. Transmission and access separated by more than two years cannot be said to be "contemporaneous by any standard."

III. Stored Communications Act, 18 U.S.C. §§ 2701–12

Owen claims that Defendants violated the Stored Communications Act (SCA), which is Title II of the Electronic Communications Privacy Act, by accessing her private emails. Those emails, she alleges, were "stored on a server at att.net."

The SCA is violated when a person "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701(a).

In their motion, Defendants first argue that the emails were not in "electronic storage" as meant in the Act, and thus Owen has not stated an SCA claim. "Electronic storage" is defined as

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
>
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; 18 U.S.C. § 2510(17).

The first definition, which concerns "temporary, intermediate storage," clearly does not apply to Owen's emails, but Defendants argue that the second definition does not apply either. Owen, Defendants point out, has not alleged that she was storing "backup" copies of her emails on the att.net server, and they cite cases in which courts have observed that email stored by a web-based email service is not stored for "backup" purposes unless another copy exists somewhere. *See Theofel v. Farey–Jones* (9th Cir. 2004) ("Even as to remote computing services that are also electronic communications services, not all storage covered by sections 2702(a)(2)(B) and 2703(b)(2)(B) is also covered by section 2510(17)(B). A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes."); *United States v. Weaver*, (C.D. Ill. 2009) ("[U]nless a Hotmail user varies from default use, the remote computing service is the only place he or she stores messages, and Microsoft is not storing that user's opened messages for backup purposes.").

But neither *Theofel* nor *Weaver* holds that an SCA claim must be dismissed if its allegations do not explicitly track one of the definitions of electronic storage in 18 U.S.C. § 2510(17). The *Theofel* court simply explained that any copies of the plaintiffs' emails stored by an electronic communication service could be considered backup copies if the plaintiffs had previously downloaded the messages. The court never suggested that, to state an SCA claim, a plaintiff must allege that a message was being stored for backup purposes. And *Weaver* involved the government's authority to subpoena certain communications in a criminal case and did not address federal civil pleading standards.

Additionally, the Court finds persuasive cases such as *Pascal Pour Elle, Ltd. v. Jin* (N.D. Ill. 2014), and *Kaufman v. Nest Seekers* (S.D.N.Y. 2006), which explicitly reject the idea that a plaintiff, to state an SCA claim, must specify that a stored electronic communication was in "temporary, intermediate storage" or was stored "for purposes of backup protection." *See Pascal* (SCA claim was adequately pled despite that plaintiff had "not alleged that the data was being stored temporarily, incidental to its transmission, or that it was stored as backup"); *Kaufman* (simple allegations that electronic communications were stored on a particular server were "sufficient to make out the element of 'electronic storage'").

Defendants next argue that, even if they accessed the emails while the emails were in electronic storage, they were authorized to do so and thus cannot be liable under the SCA. Indeed, the SCA "does not apply with respect to conduct authorized . . . by the person or entity providing a wire or electronic communications service." 18 U.S.C. § 2701(c)(1). But—unlike Defendants' undeniable authority to access the PCI computer after Owen stopped working for PCI—Defendant was not authorized to access Owen's att.net email account (at least according to Owen), and the resolution of this issue too is best reserved for consideration after discovery.

For the reasons given above, Defendants' motion to dismiss is granted in part and denied in part. Count I is dismissed without prejudice . . . and Count III may proceed.

Notes

1. This case is useful because it contrasts two complementary causes of action: the Stored Communications Act and the Wiretap Act. When faced with unauthorized access to electronic communications, first ask when the access is occurring. Is it contemporaneous with transmission (Wiretap Act) or after the fact (Stored Communications Act)?
2. In an omitted portion of the opinion, the judge addressed a Computer Fraud and Abuse Act claim related to the employer's access to the employee's old work computer. He held that the employer had the right to access the computer which, after all, it owned. Authorization is at the core of all three statutes implicated in this case. What shades of authorization are present for different kinds of employer monitoring of the computer?
3. Note that the plaintiff relies on 18 U.S.C. § 2701(a) of the Stored Communications Act, which is about accessing an Electronic Communications Service without authorization. There is not a parallel provision about accessing a Remote Computing Service without authorization, though the civil action permitted under § 2707 allows for any party aggrieved by any violation of the chapter to bring suit.

Sullinger v. Sullinger, 849 Fed.Appx. 513 (6th Cir. 2021) (unpublished)

JOHN K. BUSH, Circuit Judge.

Carol and Douglas Sullinger co-owned a software-licensing company comprised of entities including VTG Inc. and Vendita Technology Group, LLC ("VTG LLC"). She owned a 51% share of VTG LLC and served as its Manager and CEO. He owned the remaining 49% of VTG LLC and was the sole owner and president of VTG Inc. This business couple were also married. Aware that her husband was about to file for divorce, Ms. Sullinger hired VACS to install an in-home security system and another security system, including surveillance cameras, in the Vendita offices. VACS placed six pinhole cameras and small microphones in the ceiling ductwork or light fixtures in three offices; by the receptionist's desk near a common area with a copy machine; outside one office; and outside the conference room. The installation occurred after-hours during the nights of March 10 and 11, 2015. Recording took place over two days before employees discovered the cameras on or around March 13, 2015, the same day Mr. Sullinger filed for divorce. The video recordings provided no footage of him but did capture conversations of at least two employees, Chris Andrews and William Smith, recorded on March 12 and 13 in a common hallway and in another employee's office.

On March 10, 2017, while the divorce proceedings were still pending, Mr. Sullinger and VTG Inc. sued Ms. Sullinger, VACS, and John Doe in the Lucas County Court of Common Pleas. On the same day, three VTG employees—Clara Eckel, Chris Andrews, and William Smith—sued the same Defendants in another case pending in the same court. Later, Eckel voluntarily dismissed her claims, and Defendants removed both state cases to the U.S. District Court for the Northern District of Ohio.

[An epic amount of divorce related litigation is omitted here]

Trespass

The district court granted summary judgment to Defendants on the trespass claim because Ms. Sullinger had a right to possess the Vendita offices as 51% shareholder of VTG LLC at the time of the alleged trespass, and because VACS and John Doe—the surveillance company and technician who installed the equipment—acted as her agents. Thus, we affirm the district court's June 2019 order granting summary judgment to Defendants on the trespass claim.

Wiretapping

With regard to the wiretapping and invasion-of-privacy claims, Andrews and Smith point to facts that they argue suggest a factual dispute over their reasonable expectation of privacy. Specifically, they note that the record includes "some disputed" facts suggesting an expectation of privacy, such as the fact that employees changed from work clothes into gym clothes in their offices (though there was no recording of any such clothes-changing); that Ms. Sullinger did not have access to the keypad entry system for offices; that she was not permitted in the office; and that she was informed that her access code to the security system had been cancelled. The court noted some of the facts regarding Ms. Sullinger's access to the office in its analysis. Regardless, none of those facts establishes a genuine dispute of *material* fact. What matters is that the conversations were recorded in a common space or another employee's office and that Ms. Sullinger was still a majority owner of the business. As explained below, these facts establish as a matter of law that there was no violation of the federal and state wiretapping statutes and no tortious invasion of privacy with respect to the particular recordings that were made.

The district court held that Andrews and Smith had no expectation of privacy in the shared spaces of the office or in another employee's office. The federal wiretapping statute protects "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation," except for electronic communications. The Ohio statute provides a nearly identical definition of "oral communications." We have adopted a two-part reasonable-expectation test to determine if an oral communication is protected, considering whether (1) "a person exhibited an expectation of privacy," and (2) "whether that expectation was reasonable." The first prong is not met if a person either "*exposes* . . . statements to the 'plain view' of outsiders" or "fails to take . . . steps to prevent exposure to third parties." For the second prong, we ask whether "society is prepared to recognize an exhibited expectation as legitimate." An "employee has a reasonable expectation of privacy in his office." *Bender's, Inc. v. Walker* (6th Cir. 2001) (stating so in the Fourth Amendment context). And employees can have a reasonable expectation of privacy in the workplace where employees "take care to ensure that their conversations remained private" in a "small, relatively isolated" shared office.

The facts that Andrews and Smith assert are in dispute are not material under the standard for whether an employee has a reasonable expectation of privacy. They do not dispute the facts that they were recorded in a common hallway and in another employee's office and that in both places, they could easily be overheard and exhibited no intent to keep their conversations private. It would be one thing if the conversations had taken place in an arguably

private spot, such as perhaps one of those employees' workstations, or if the cameras had recorded speech or conduct as to which the employees had a reasonable expectation of privacy. But these conversations were not in private. They were open, in a common space where others could hear them. Thus, the employees could not have had a reasonable subjective belief that Ms. Sullinger, a majority shareholder of VTG LLC, would not learn of their conversations. Therefore, the district court properly granted summary judgment on these claims.

Invasion-of-Privacy Claims

The district court held that the Andrews' and Smith's claims for invasion of privacy failed because (1) they "had no reasonable expectation that the owner of their company could not listen to their communications in open hallways or through [the other employee's] open door;" and (2) "there is no evidence that Carol disclosed the recordings to anyone." The Supreme Court of Ohio has held that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." A plaintiff must raise facts showing that a defendant "wrongful[ly] intru[ded] into" the plaintiff's "private activities." Whether a plaintiff's activities were "private" depends on whether he has a reasonable expectation of privacy based on the totality of circumstances.

Andrews and Smith argue that they had a reasonable expectation of privacy under the circumstances, raising the same facts that underlie the wiretapping claims. Although the test for determining whether a plaintiff had a reasonable expectation of privacy in the invasion-of-privacy context does not precisely mirror that for wiretapping claims, the same reasoning applies here. As discussed above, Andrews and Smith were recorded in a common space and in another employee's office where they could be easily overheard, outside their immediate workspaces, in the workplace of a business that Ms. Sullinger co-owned. Thus, the district court was correct to hold that they had no reasonable expectation of privacy.

Notes

1. Not every interception of an oral communication can be the subject of a wiretap claim; there must be an expectation of privacy in the communication. That piece of doctrine is clear enough from the text of the statute, but was the court right in how it applied it to these facts? Is this outcome wrong? Right only because the defendant was a partial owner of the space? Right in general because office hallways are not private?
2. Because of the close parallel between the wiretap claim and the intrusion upon seclusion claim, consider the role of the ECPA in establishing damages. A successful ECPA claim may be worth tens of thousands of dollars. A successful intrusion upon seclusion claim—absent concrete injury or obviously embarrassing revelations—may be worth far less.

Democracy Partners v. Project Veritas Action Fund, 285 F.Supp.3d 109 (D.D.C. 2018)

ELLEN SEGAL HUVELLE, United States District Judge

Democracy Partners, LLC, Strategic Consulting Group, NA, Inc., and Robert Creamer bring this action against Project Veritas Action Fund, Project Veritas, James O'Keefe ("PV defendants"), and Allison Maass, alleging that defendants violated federal and state wiretap statutes and committed multiple common law torts in their execution of an undercover sting operation directed at plaintiffs.

Democracy Partners, LLC, is "a company including a number of other consultants and vendors to progressive organizations and Democratic campaigns and committees, who market their services collectively through the company." "Democracy Partners' private offices . . . are not accessible to the general public, have 24–hour security, and are only accessible if one signs into the building at the lobby security desk, if one is provided entrance by [p]laintiffs' receptionist, and/or if one has an electronic pass card[, which] . . . is required to access the

elevators to the office outside of regular business hours[,] and a key[, which] is required to enter the office when no one is present."

On or about June 24, 2016, Sandini, using the false name of Charles Roth and representing himself as a potential donor to a nonprofit organization that Creamer had worked for, was introduced to Creamer and the two men had a meeting. A few weeks later, on or about July 15, 2016, Sandini "told Creamer that he had a niece who wanted to volunteer to do some kind of political work for Democratic candidates or organizations while she was on a brief hiatus from college." Sandini told Creamer that his niece's name was "Angela Brandt." In reality, no such person existed; rather, Angela Brandt was a false name used by Maass.

In late August 2016, Sandini called Creamer and told him that his niece would like to gain more experience, leading Creamer to interview Maass "for an internship with Creamer and Strategic in the Democracy Partners office." During the interview, Maass provided Creamer fictitious background information and falsely "told Creamer that her interest in obtaining an internship was to gain work experience in political and advocacy work."

On September 21, 2016, Maass started her internship at Democracy Partners. She was given an electronic pass card, which allowed her access to the entire office at all times, "including areas that contained file cabinets and computers with confidential information," and an account and password allowing her to use a company computer.

During her internship, unbeknownst to plaintiffs, Maass carried concealed video and audio recording devices. She secretly recorded her discussion with Creamer on her first day of work, along with "other confidential internal conversations with Creamer and other Democracy Partners members, as well as confidential conversations they had with [Strategic] and Democracy Partner clients in-person and via conference call." She provided these unauthorized audio and video recordings to PV and PVAF. Without permission, she also provided them with a number of confidential documents and emails.

On October 14, 2016, Creamer went to lunch with Mike Carlson, whom Sandini had falsely claimed was his financial advisor. Just as they were finishing, Creamer was accosted by a reporter, Raffi Williams, and a film crew from Circa Media, a subsidiary of Sinclair Broadcasting, who asked him to respond to two secretly recorded video clips of Creamer. The reporter indicated that O'Keefe had been the one to tip him off to Creamer's whereabouts. When Creamer returned to his office, Maass was no longer there, and she never returned.

On October 17, 18, 24 and 26th, however, PVAF released a series of videos to PV's YouTube channel that contained footage from Maass' recordings of Creamer, Democracy Partners, and its clients.

Unauthorized Entry [Trespass Claim]

In *Council on American–Islamic Relations Action Network, Inc. v. Gaubatz* (D.D.C. 2011) ("*CAIR 2011*"), the court denied a motion to dismiss a claim of trespass brought against an intern who obtained his job—and thus his consent to enter defendants' offices—through fraud and subterfuge. *See CAIR 2011*; *see also Planned Parenthood Fed'n v. Ctr. for Medical Progress* (N.D. Cal. 2016) (allowing trespass claim to proceed where the defendants obtained consent to enter non-publicly accessible property through misrepresentation). The situation in the present case is indistinguishable from *CAIR 2011*. The complaint alleges that Maass obtained her job—and thus the consent to enter Democracy Partners' office—through misrepresentation. Under these circumstances, plaintiffs "consent" does not bar a claim for trespass.

In the alternative, even if Maass' misrepresentation does not vitiate plaintiffs' consent to her entry, the complaint also alleges that Maass exceeded the scope of any consent by secretly recording conversations in Democracy Partners' office to turn over to the PV defendants. That allegation is also sufficient to state a claim for trespass.

Wiretap Claims

Under both the Federal Wiretap Act and the D.C. Wiretap Act, a person may be liable if he or she

> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> . . .
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; [or]
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; . . .
>
> 18 U.S.C. §§ 2511(1); *see* D.C. Code § 23–541(a)(1) (similar provision).

The complaint alleges that Maass "willfully intercepted the oral communications of Plaintiffs and their employees by using an electronic device concealed on her person to make video and audio recordings of conversations and meetings involving Plaintiffs and their employees and clients pertaining to Plaintiffs' confidential affairs and activities" [and that such recordings were disclosed].

The PV defendants do not challenge the adequacy of the above allegations, but they argue that both wiretap claims should be dismissed because there is a "one-party consent" exception to liability in both statutes that protects Maass' recordings. In the Federal Wiretap Act, that exception provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State. 18 U.S.C. § 2511(2)(d).

The D.C. Wiretap Act similarly provides that "[i]t shall not be unlawful under this section for—(3) a person not acting under color of law to intercept a wire or oral communication, where such person is a party to the communication . . . unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States, any State, or the District of Columbia, or for the purpose of committing any other injurious act." D.C. Code § 23–542(d)(3). The PV defendants assert that Maass' recordings are covered by these exceptions because (1) Maass was a "party" to each recorded communication; and (2) the complaint does not plausibly allege a criminal or tortious purpose.

To plausibly allege a criminal or tortious purpose requires "'either (1) that the primary motivation, or (2) that a determinative factor in the actor's motivation in intercepting the conversation was to commit' a criminal or tortious act." The complaint alleges that the communications were intercepted "for the primary purpose of committing trespass, breach of fiduciary duty, fraudulent misrepresentation and other criminal or tortious acts."

But the Court does not agree that a "determinative factor" in making the recordings could not have been to commit a breach of fiduciary duty. First, the Court has already rejected

defendants' primary contention that the complaint does not adequately allege the existence of a fiduciary duty. *See Planned Parenthood* (denying motion to dismiss claim under Federal Wiretap Act where complaint plausibly alleged at least one tortious act after the interception). Second, despite the PV defendants' assertion that their "immediate purpose" at the time the recordings were made was something other than what plaintiffs allege, that is not something the Court can consider at this stage of the proceedings. *See also CAIR v. Gaubatz* (D.D.C. 2014) (allowing similar claim to proceed at summary judgment stage because "if [the intern] understood himself to be bound by a fiduciary duty of non-disclosure, then it appears obvious that the breach of this fiduciary duty was the primary motivation, or at least a motivating factor, in his interception of the communications at issue").

As plaintiffs have plausibly alleged at least one tortious purpose that occurred after the interception, the one-party consent defense does not provide a basis for dismissing the wiretap claims.

Notes

1. This is an unusual case in that it effectively involves the privacy of the employer from the employee. Think about it in relation to *Sullinger*. Is it consistent to protect the privacy of the employer here, but not the employee in *Sullinger*? Should both kinds of monitoring be permitted? Neither?

2) Cameras in the workplace

Employers are generally permitted to record employee activities in public areas. Still, courts are willing to recognize intrusion upon seclusion claims stemming from employer video surveillance in some contexts.[229] Specifically, courts may uphold intrusion upon seclusion claims when cameras are placed in bathrooms, break rooms, locker rooms, or private offices even if the cameras do not record particularly private conduct.[230]

State statutes limiting video surveillance in the workplace primarily focus on areas with unique privacy interests.[231] In particular, surveillance of bathrooms and places of comfort where business is not being conducted (such as employee break rooms) may be limited. Additionally, state and federal labor laws can prevent employers from interfering with employee bargaining through video surveillance.

Two states with notable laws are New York and Connecticut. New York's law is relatively narrow: "No employer may cause a video recording to be made of an employee in a restroom, locker room, or room designated by an employer for employees to change their clothes, unless authorized by court order."[232] The law provides for civil action against violators and seeks to prevent employers from using video gathered by illegal surveillance.[233]

Connecticut also limits employers' use of electronic surveillance. Specifically, the law states that "[n]o employer or agent or representative of an employer shall operate any electronic surveillance device or system, including but not limited to the recording of sound or voice or a closed circuit television system, or any combination thereof, for the purpose of recording or

---

[229] 6 EMP. COORDINATOR EMP. PRACS. *Video surveillance of employees* § 55:3, Westlaw (database updated Feb. 2024).

[230] *Koeppel v. Speirs*, 779 N.W.2d 494 (Iowa Ct. App. 2010); *Hernandez v. Hillsides, Inc.*, 47 Cal.4th 272 (Cal. 2009).

[231] 6 EMP. COORDINATOR EMP. PRACS. *Video surveillance of employees* § 55:3, Westlaw (database updated Feb. 2024).

[232] N.Y. LAB. LAW § 203-c (McKinney 2021).

[233] *Id.*

monitoring the activities of his employees in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as restrooms, locker rooms or lounges."[234] Additionally, the statute protects labor negotiations from employer monitoring by stating "[n]o employer or his agent or representative and no employee or his agent or representative shall intentionally overhear or record a conversation or discussion pertaining to employment contract negotiations between the two parties, by means of any instrument, device or equipment, unless such party has the consent of all parties to such conversation or discussion."[235]

These statutes are notable for their limited scope. Each prevents video recording in places where, realistically, we all know video recording should not occur. But it is only because of the clarity of the statutes that we know video recording is impermissible in these locations. One could imagine arguing that an employee locker room should have video monitoring, to prevent theft both from and by employees. One could even imagine a judge considering that video monitoring reasonable—or at least not highly offensive—if safeguards were adopted. Some states, however, foreclose that argument.

3) GPS monitoring of vehicles

Another major issue that is governed by state law is GPS tracking. Employers often have an interest in monitoring the physical locations and driving behavior of their employees during the workday. States generally permit this, but some require the consent of the person being tracked.[236]

Two state statutes of note are New Jersey's and Indiana's. First, New Jersey restricts employers from tracking employees without notice. The law states that "[a]n employer who knowingly makes use of a tracking device in a vehicle used by an employee without providing written notice to the employee shall be subject to a civil penalty in an amount not to exceed $1,000 for the first violation and not to exceed $2,500 for each subsequent violation . . . ."[237]

Indiana, by contrast, prohibits placing a "tracking device on an individual or on property owned or used by an individual, without the knowledge or consent of the individual," making it a Class A misdemeanor.[238] But there are exceptions for a "person who places a tracking device on property in which the person has an ownership or contractual interest, unless the person is the subject of a protective order and the property is likely to be used by the person who obtained the protective order" and a "device installed as original equipment by the manufacturer of a motor vehicle." This means that an employer can track an employer-owned vehicle *without* the knowledge or consent of the individual expected to drive it, but the employer would need consent to track an employee-owned vehicle.

Notably it is not difficult for employers to give notice and get consent in most states. An employer could put in the employee handbook that they monitor the location of vehicles during work hours and this would be sufficient under New Jersey law, especially if the employee had to sign an acknowledgement that they had read the policy. More generally, private employers are typically permitted to track employer-owned cars and state courts are unwilling to recognize GPS monitoring of employer-owned/leased vehicles as grounds for an intrusion upon seclusion

---

[234] CONN. GEN. STAT. ANN. § 31-48b.

[235] *Id.*

[236] Robert Sprague, *Privacy Self-Management: A Strategy to Protect Worker Privacy from Excessive Employer Surveillance in Light of Scant Regulations*, 60 AM. BUS. L.J. 793, 815 (2023) (collecting thirteen state statutes on this point).

[237] N.J. STAT. § 34:6B-22.

[238] IND. CODE § 35-46-8.5-1.

claim.[239] For example, one court held "Use of the tracking device on defendant's company car, even though it was assigned to plaintiff, does not constitute a substantial intrusion upon plaintiff's seclusion, as it revealed no more than highly public information as to the van's location. Especially because the van was the property of defendant, defendant's use of the tracking device on its own vehicle does not rise to the level of being highly offensive to a reasonable person." *Elgin v. St. Louis Coca-Cola Bottling Co.*, 2005 WL 3050633, at *4 (E.D. Mo. Nov. 14, 2005).

The one caveat to this general rule is that the employer must sometimes provide a legitimate business reason for GPS tracking. For example, Florida law prohibits use of tracking applications but includes an exemption for a "person acting in good faith on behalf of a business entity for a legitimate business purpose."[240]

Cunningham v. New York State Department of Labor, 997 N.E.2d 468 (N.Y. 2013)

SMITH, J.

The State of New York, suspecting that one of its employees was submitting false time reports, attached a global positioning system (GPS) device to the employee's car. We hold that the search did not require a warrant, but that on the facts of this case it was unreasonable.

Petitioner became a state employee in 1980, and in 1989 was appointed as Director of Staff and Organizational Development of the State Department of Labor. In 2008, the Department began an investigation relating to petitioner's alleged unauthorized absences from duty and the falsification of records to conceal those absences. That investigation led to a disciplinary proceeding that resulted in a two-month suspension; it also led to a second investigation, because, after petitioner eluded an investigator who was following his car, the Department referred petitioner's conduct to the Office of the State Inspector General. The Inspector General's investigation resulted in a second disciplinary proceeding, the one now before us.

As far as the record shows, the first step in the Inspector General's investigation was to attach a GPS device to petitioner's car, without petitioner's knowledge, while the car was parked in a lot near the Department of Labor offices. This device and two later replacements recorded all of the car's movements for a month, including evenings, weekends and several days when petitioner was on vacation in Massachusetts. Later, the Inspector General pursued other avenues of investigation: surveillance of an apartment building petitioner was suspected of visiting during working hours, subpoenas for E–ZPass records and interviews of petitioner and his secretary.

After receiving the Inspector General's report, the Department brought new charges against petitioner, of which 11 were sustained by a Hearing Officer. As to three charges, the GPS information showed that petitioner's times of arrival at and departure from his office were inconsistent with the number of hours he claimed, on time records he submitted, to have worked. A fourth charge was based on petitioner's approval of time records showing his secretary was working during hours when the GPS information showed that he was visiting her home.

We decided in *People v. Weaver* (N.Y. 2009), and the Supreme Court decided in *United States v. Jones* (2012), that the attachment by law enforcement officers of a GPS device to the automobile of a criminal suspect, and the use of that device to track the suspect's movements, was a search subject to constitutional limitations. Here, the State argues, and we agree, that

---

[239] Sprague, *supra* note 239, at 813; HUM. RES. GUIDE *GPS monitoring: The legal issues* § 5:120, Westlaw (database updated Nov. 2023).

[240] FLA. STAT. ANN. § 934.425(d).

this search is within the "workplace" exception to the warrant requirement recognized in *O'Connor v. Ortega* (1987). Petitioner here does not challenge the existence of a workplace exception to the warrant requirement, but argues that it is inapplicable because the object of the search in this case was petitioner's personal car.

The *O'Connor* plurality observed that such items as a personal photograph on an employee's desk, or a personal letter posted on an employee bulletin board, are part of the workplace. The location of a personal car used by the employee during working hours does not seem to us more private. Petitioner was required to report his arrival and departure times to his employer; this surely diminished any expectation he might have had that the location of his car during the hours he claimed to be at work was no one's concern but his. We are unpersuaded by the suggestion in the concurring opinion that, on our reasoning, a GPS device could, without a warrant, be attached to an employee's shoe or purse. People have a greater expectation of privacy in the location of their bodies, and the clothing and accessories that accompany their bodies, than in the location of their cars.

The reasons that led the *O'Connor* Court to dispense with the warrant requirement—the serious disruption that such a requirement would entail, and the burden it would impose on supervisors who "are hardly in the business of investigating the violation of criminal laws"—apply no less to an investigation of the kind at issue here than to the investigations in *O'Connor* and in *Ontario v. Quon* (2010), which involved a scrutiny of text messages on an employer-issued pager. We thus conclude that when an employee chooses to use his car during the business day, GPS tracking of the car may be considered a workplace search.

The Inspector General did not violate the State or Federal Constitution by failing to seek a warrant before attaching a GPS device to petitioner's car.

While the search did not require a warrant, it did not comply with either the State or Federal Constitution unless it was a reasonable search. We conclude that the State has failed to demonstrate that this search was reasonable.

The *O'Connor* plurality summarized the approach of courts to the question of reasonableness in this way:

> "Determining the reasonableness of any search involves a twofold inquiry: first, one must consider whether the action was justified at its inception; second, one must determine whether the search as actually conducted was reasonably related in scope to the circumstances which justified the interference in the first place . . . .
>
> "The search will be permissible in its scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct."

Under *O'Connor,* a workplace search based on a reasonable suspicion of employee misconduct is "justified at its inception." The search in this case clearly meets that test. Petitioner's employer had ample grounds to suspect him of submitting false time records.

We cannot find, however, that this search was reasonable in its scope. It was, in the words of the *New York v. T.L.O.* (1985) Court quoted in *O'Connor,* "excessively intrusive." It examined much activity with which the State had no legitimate concern—i.e., it tracked petitioner on all evenings, on all weekends and on vacation. Perhaps it would be impossible, or unreasonably difficult, so to limit a GPS search of an employee's car as to eliminate all surveillance of private activity—especially when the employee chooses to go home in the middle of the day, and to conceal this from his employer. But surely it would have been possible to stop short of seven-day, 24–hour surveillance for a full month. The State managed to remove a GPS device from petitioner's car three times when it suited the State's convenience to do so—twice to replace it with a new device, and a third time after the surveillance ended. Why could it not

also have removed the device when, for example, petitioner was about to start his annual vacation?

It is true that none of the evidence used against petitioner in this case resulted from surveillance outside of business hours. Where an employer conducts a GPS search without making a reasonable effort to avoid tracking an employee outside of business hours, the search as a whole must be considered unreasonable. That conclusion concededly requires suppression of the GPS evidence here; the State has disclaimed any reliance on the balancing test that we use when deciding whether to invoke the suppression remedy in administrative proceedings.

The consequence of suppression in this case is not to preclude the State from disciplining petitioner. As the majority and the dissenting Justices in the Appellate Division agreed, only four of the 11 counts on which petitioner was found guilty depended on GPS evidence, and only those four charges need be dismissed. As to the others, the GPS evidence was either substantially duplicated by E–ZPass records or was wholly irrelevant. Whether the seven surviving charges warrant the same or a lesser penalty is a matter to be decided, in the first instance, by the Commissioner of Labor on remand.

Accordingly, the judgment of the Appellate Division should be reversed, with costs, charges one, two, three and six against petitioner dismissed, and the matter remitted to the Appellate Division with directions to remand to the Commissioner of Labor for redetermination of the penalty.

ABDUS–SALAAM, J. (concurring).

I would hold that the State cannot, without a warrant, place a GPS on a personal, private car to investigate workplace misconduct.

In *Weaver,* we explained that GPS tracking is more intrusive than simply following a car, and that GPS surveillance is not analogous to visual surveillance for the purposes of constitutional analysis. It took "little imagination" for us to conjure the types of "indisputably private" information that would be "[d]isclosed in the data" from a GPS device planted on a person's vehicle.

Recognizing that, "[w]ithout judicial oversight, the use of [GPS] devices presents a significant and, to our minds, unacceptable risk of abuse" (*Weaver*), we held that "[u]nder our State Constitution . . . the installation and use of a GPS device to monitor an individual's whereabouts requires a warrant supported by probable cause."

The privacy and constitutional concerns recognized in *Weaver* and *Jones* apply equally in this case. Surely, a government employer's interest in determining whether its employees are falsifying time records is just as important as the State's interest in protecting the public from dangerous criminals. Yet, the majority, ignoring our concerns in *Weaver,* would permit government employers who suspect employees of misconduct to use GPS devices, without first obtaining a warrant, to track and monitor those employees' precise whereabouts during business hours.

The potential dangers of the majority's decision are evident when one considers a government employee, suspected of falsifying time records, who does not drive a car during the workday, but instead leaves the office on foot or takes public transit. There is now little to prevent a government employer from placing a GPS device on that person's bag, briefcase, shoe, cell phone, watch, or purse—anything that is used during the workday (like petitioner's car)—to determine whether, based on the tracking data transmitted by that device, the employee is located where he or she purports to be. The majority's statement that people have a greater expectation of privacy in the location of their bodies than in the location of their cars avoids addressing the point that petitioner's employer was using electronic surveillance to track *petitioner's* location; tracking his personal car was only a means to that end.

The ramifications of the majority's decision will extend far beyond this case. All government employees, at all levels, in all three branches of government, may now be subject to electronic surveillance based upon a mere "reasonableness" standard, without any judicial oversight at the inception of the search. Given the majority's imprimatur of warrantless GPS tracking, less intrusive methods for investigating government employees will almost certainly be replaced with electronic surveillance. The potential for abuse that we recognized in *Weaver* is now closer to becoming a reality.

Notes

1. Although *Cunningham* dealt with a public employer, lawyers will recommend that GPS tracking of a private employee's private vehicle similarly be limited only to business hours.[241]
2. One industry deeply interested in GPS tracking is long-distance trucking. Trucking companies—which sometimes but not always own the vehicles being used—have a strong interest in knowing where the trucks and loads are at any given moment. They also have mixed incentives regarding the monitoring of truck driver safety. Though driver and truck safety is important, protection of them can come at a major cost. Federal trucking regulations put limits on the amount of hours a person can drive. Strict adherence to these regulations would sometimes leave loads awkwardly short of their destinations, costing companies and drivers money. Prior to the advent of electronic tracking, it was common for drivers to lie on the paper records they kept to make sure that loads could get where they needed to be. Electronic tracking makes this kind of deception difficult, to the aggravation of some drivers and some companies.[242]

4) Drug testing

Employee drug testing remains one way in which private and public employers monitor employee behavior. Typically, private employers are permitted to engage in employee drug testing subject to statutory limitations.[243] State courts generally do not recognize employee drug testing as an intrusion upon seclusion.

States vary on whether they have statutes regarding employee drug testing. Most permit employers to require employee drug testing within limitations of varying strictness. Many states require employers to give notice of drug testing policies and place restrictions on the purposes behind these tests. Additionally, state laws sometimes prevent disclosure of test results by employers. Another note is that every state permits drug testing for positions that engage in the care of individuals or where incapacitation could pose a risk to the broader public.

Two states with notable statutes are Minnesota and Connecticut. Minnesota prohibits employers from requiring drug or alcohol testing of employees unless it is for a job candidate with an offer, routine physical examination, under reasonable suspicion, or the employee is undergoing treatment.[244] Additionally, Minnesota distinguishes between cannabis testing and other illicit drug testing. The law permits cannabis testing only for "a safety-sensitive position,"

---

[241] GUIDE TO HR POL'YS & PROCS. MANUALS *GPS monitoring* § 7:59, Westlaw (database updated Jan. 2024); HUM. RES. GUIDE *GPS monitoring: The legal issues* § 5:120, Westlaw (database updated Nov. 2023); Annie Villanueva Jeffers & Crystal D. Barnes, *Every Move You Make: When Monitoring Employees Gives Rise to Legal Risks*, SKADDEN INSIGHTS (Sept. 2022), https://www.skadden.com/insights/publications/2022/09/quarterly-insights/every-move-you-make.

[242] *See, e.g.*, KAREN LEVY, DATA DRIVEN: TRUCKERS, TECHNOLOGY, AND THE NEW WORKPLACE SURVEILLANCE (2022).

[243] LEXISNEXIS 50 STATE SURVS.: STATUTES & REGULS., *Labor & Employment Law – Employee Privacy: Drug & Alcohol Testing* (February 2023).

[244] MINN. STAT. § 181.951.

"a peace officer position," "a firefighter position," "a position requiring face-to-face care, training, education, supervision, counseling, consultation, or medical assistance to children, vulnerable adults, or patients who receive health care services from a provider for the treatment, examination, or emergency care of a medical, psychiatric, or mental condition."

Connecticut prohibits employers from making employment decisions based on a positive drug test result unless "(1) the employer has given the employee a urinalysis drug test, utilizing a reliable methodology, which produced a positive result and (2) such positive test result was confirmed by a second urinalysis drug test, which was separate and independent from the initial test, utilizing a gas chromatography and mass spectrometry methodology or a methodology which has been determined by the Commissioner of Public Health to be as reliable or more reliable than the gas chromatography and mass spectrometry methodology."[245]

Moreover, Connecticut law states in regard to non-random drug tests that "[n]o employer may require an employee to submit to a urinalysis drug test unless the employer has reasonable suspicion that the employee is under the influence of drugs or alcohol which adversely affects or could adversely affect such employee's job performance."[246] Still, Connecticut does permit random drug tests if "(1) such test is authorized under federal law, (2) the employee serves in an occupation which has been designated as a high-risk or safety-sensitive occupation pursuant to regulations adopted by the Labor Commissioner pursuant to chapter 54, or is employed to operate a school bus or a student transportation vehicle, or (3) the urinalysis is conducted as part of an employee assistance program sponsored or authorized by the employer in which the employee voluntarily participates."[247]

Although employee drug testing does not violate intrusion upon seclusion, state courts are willing to recognize torts for public disclosure of private facts if the employer reveals positive drug test results. When an employer discloses a positive drug test to the public, it can be considered an actionable offense. Some state statutes require employers to treat drug test results as medical information and thus not disclose the result, even if the employment action is motivated by a positive test.[248]

---

[245] CONN. GEN. STAT. § 31-51u.
[246] CONN. GEN. STAT. § 31-51x.
[247] *Id.*
[248] 28 AM. JUR. PROOF OF FACTS 3d 185, §§ 21–22 (Originally published in 1994).

XII. European Privacy Law

A. The European Convention on Human Rights 619
Von Hannover v. Germany, No. 59320/00, Eur. Ct. H.R 294 (2004) 621

B. The Data Protection Directive and the Right to be Forgotten 630
Google Spain SL v. Agencia Española de Protección de Datos (AEPD), No. C-131/12, E.C.J. (2014) 630

C. Basic Features of the General Data Protection Regulation 639
Bundesverband der Verbraucherzentralen und Verbraucherverbände v. Planet49 GmbH, No. C-673/17, E.C.J. (2019) 643
Meta v Bundeskartellamt, No. C-252/21, E.C.J. (2023) 649

D. GDPR and International Data Transfers.....657
Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximilian Schrems (*Schrems II*), No. C-311/18, E.C.J. (2020) 658

The focus of this book is on American privacy law and this chapter, standing alone, will not do much to change that. Yet studying European privacy law shows us that the American approach to privacy is not the only possible approach. In Europe, somewhat different norms and somewhat different values lead to somewhat different regulations. These regulations are then applied to citizens and consumers who are, broadly speaking, quite like Americans. If it works over there (which some argue it does not), then it could work over here (which some would argue would be bad).

Pretty much everyone thinks that the United States is due for a major reform of privacy law. If there is an article praising the current patchwork system of laws as a comprehensive solution to privacy regulation, I have not found it. Since we are due to reconsider our basic approach to privacy, what can we learn from Europe's approach to privacy law? Which of their ideas are good, which are bad, and which would be entirely unconstitutional if implemented in the United States?

Much discussion of transatlantic differences in privacy law presumes that there is some great philosophical gulf between Americans and Europeans. The legal theorist James Q. Whitman wrote an excellent book describing the different cultures of criminal punishment in the United States and in Europe, and then followed it up with a widely-cited *Yale Law Journal* piece doing much the same analysis in regard to privacy law.[249] In his view, the American approach to privacy is fundamentally concerned with liberty from the state whereas the European approach is fundamentally concerned with protecting dignity from private intrusion. That one word, "dignity," does a lot of heavy lifting in European privacy theorizing.

In the penal context, I think Whitman is wrong. Everyday Americans and Europeans have fairly similar attitudes toward criminal sentencing.[250] The massive difference in incarceration policy outcomes between the United States and every other industrialized democracy is much more likely due to the structure of our criminal justice system than the

---

[249] HARSH JUSTICE: CRIMINAL PUNISHMENT AND THE WIDENING DIVIDE BETWEEN AMERICA AND EUROPE (Oxford Univ. Press 2003); *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

[250] Matthew B. Kugler, Friederike Funk, Judith Braun, Mario Gollwitzer, Aaron C. Kay & John M. Darley, *Differences in Punitiveness Across Three Cultures: A Test of American Exceptionalism in Justice Attitudes*, 103 J. CRIM. L. & CRIMINOLOGY 1071 (2013).

attitudes of our people. Perhaps in a later edition of this book I will include an excerpt here from a future article testing his theories in the privacy space. But I have not written that article yet, so you must wait.

As you read through this chapter, consider the extent to which the European approach is representative of different values than the American approach. If you were told that a particular European regulation was the law of some new U.S. state—perhaps the state of East Virginia—would you be surprised?

A. The European Convention on Human Rights

Speaking of "European" privacy law is difficult because there is no single definition of Europe. Arguably Russia is a European country—despite mostly being in Asia—and Switzerland definitely is, but neither has adopted the General Data Protection Regulation nor is a member of the European Union (EU). So "Europe" as used here is always going to refer to the portion of Europe that has signed on to whichever agreement is currently being discussed.

Given where European privacy law has gone over the past several generations, the best place to start this discussion is with the European Convention on Human Rights. The European Convention on Human Rights was created by the Council of Europe, an international organization that was born in the U.S.-aligned portions of Western Europe at the end of World War II. The purpose of the organization was to uphold human rights, democracy, and the rule of law in Europe. After the end of the Cold War, the Council ultimately grew to encompass all of Europe save Russia and Belarus.

The Council of Europe drafted the Convention on Human Rights in 1950 and the Convention came into effect in 1953. Its purpose was to both articulate a general charter of human rights and also to create a legal mechanism by which the citizens of the member states could enforce those rights. To this end, the Convention is enforced by the European Court of Human Rights.

Two of the Articles of the Convention are directly relevant to privacy and data protection. Specifically:

> **Article 8 – Right to respect for private and family life**
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
>
> **Article 10 – Freedom of expression**
>
> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in

> the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

There are several things to note about these two Articles. To begin, compare them to U.S. Constitution. U.S. protection for freedom of expression stems from the First Amendment: "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." Despite covering several more topics than Article 10, it is far shorter. It is also absolute: Congress shall make *no law*. Article 10, by contrast, looks like weak tea. It has endless exceptions and states that freedom of expression brings with it "duties and responsibilities."

Yet this difference is one of form rather than substance. One could easily put U.S. Supreme Court case citations after every clause in Paragraph 2 of Article 10 that limits the freedom of speech. European drafters simply tend to write laws in a different style than do American drafters. Though there are differences between European and American freedom of speech—American freedom of speech is more absolute, despite its many exceptions—mere text is not the source of them.

More substantively, Article 8 has no obvious parallel in the U.S. Constitution. Consider the various disputes over whether the Constitution even protects privacy, let alone what privacy it might protect. In contrast, the Convention simply states that everyone shall have privacy protection. It even lists this right before freedom of expression, if one wants to read importance from order.

This dual interest in privacy and freedom of expression was also enshrined decades later in the Charter of Fundamental Rights of the European Union (2000).

> **Article 7: Respect for private and family life**
>
> Everyone has the right to respect for his or her private and family life, home and communications.
>
> **Article 8: Protection of personal data**
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.
>
> **Article 11: Freedom of expression and information**
>
> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
>
> 2. The freedom and pluralism of the media shall be respected.

Though most actual practice of European privacy law concerns privacy statutes rather than these core provisions, they are still foundational. A series of cases involving Princess Caroline von Hannover of Monaco illustrate the role the European Court of Human Rights plays in this area and also sets the stage for later statutory regulation, including GDPR. The case is

Von Hannover v. Germany (as opposed to some private party) because Princess Caroline's fundamental complaint was that German law was insufficiently protective of her privacy.

Note: European court decisions are often available in multiple languages. The version of English used by European courts employs British English. British spelling is preserved in these excerpts.

Von Hannover v. Germany, No. 59320/00, Eur. Ct. H.R 294 (2004)

1. The case originated in an application against the Federal Republic of Germany lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a national of Monaco, Caroline von Hannover ("the applicant"), on 6 June 2000.

2. The applicant alleged that the German court decisions in her case had infringed her right to respect for her private and family life as guaranteed by Article 8 of the Convention.

8. The applicant, who is the eldest daughter of Prince Rainier III of Monaco, was born in 1957. Her official residence is in Monaco but she lives in the Paris area most of the time.

As a member of Prince Rainier's family, the applicant is the president of certain humanitarian or cultural foundations, such as the Princess Grace Foundation or the Prince Pierre of Monaco Foundation, and also represents the ruling family at events such as the Red Cross Ball or the opening of the International Circus Festival. She does not, however, perform any function within or on behalf of the State of Monaco or any of its institutions.

9. Since the early 1990s the applicant has been trying—often through the courts—in a number of European countries to prevent the publication of photos about her private life in the tabloid press.

10. The photos that were the subject of the proceedings described below were published by the Burda publishing company in the German magazines *Bunte* and *Freizeit Revue*, and by the Heinrich Bauer publishing company in the German magazine *Neue Post*.

1. The first series of photos

(a) The five photos of the applicant published in *Freizeit Revue* magazine (issue no. 30 of 22 July 1993).

11. These photos show her with the actor Vincent Lindon at the far end of a restaurant courtyard in Saint-Rémy-de-Provence. The first page of the magazine refers to "The most tender photos of her romance with Vincent" and the photos themselves bear the caption "These photos are evidence of the most tender romance of our time."

(b) The two photos of the applicant published in *Bunte* magazine (issue no. 32 of 5 August 1993).

12. The first photo shows her on horseback with the caption "Caroline and the blues. Her life is a novel with innumerable misfortunes, says the author Roig." The second photo shows her with her children Pierre and Andrea. The photos are part of an article entitled "I don't think I could be a man's ideal wife."

(c) The seven photos of the applicant published in *Bunte* magazine (issue no. 34 of 19 August 1993).

13. The first photo shows her canoeing with her daughter Charlotte, the second shows her son Andrea with a bunch of flowers in his arms. The third photo shows her doing her shopping with a bag slung over her shoulder, the fourth with Vincent Lindon in a restaurant and the fifth alone on a bicycle. The sixth photo shows her with Vincent Lindon and her son

Pierre. The seventh photo shows her doing her shopping at the market, accompanied by her bodyguard. The article is entitled "Pure happiness."

2. The second series of photos

(a) The ten photos of the applicant published in *Bunte* magazine (issue no. 10 of 27 February 1997).

14. These photos show the applicant on a skiing holiday in Zürs/Arlberg. The accompanying article is entitled "Caroline . . . a woman returns to life."

(b) The eleven photos of the applicant published in *Bunte* magazine (issue no. 12 of 13 March 1997).

15. Seven photos show her with Prince Ernst August von Hannover at a horse show in Saint-Rémy-de-Provence. The accompanying article is entitled "The kiss. Or: they are not hiding anymore." Four other photos show her leaving her house in Paris with the caption "Out and about with Princess Caroline in Paris."

(c) The seven photos of the applicant published in *Bunte* magazine (issue no. 16 of 10 April 1997).

16. These photos show the applicant on the front page with Prince Ernst August von Hannover and on the inside pages of the magazine playing tennis with him or both putting their bicycles down.

3. The third series of photos

17. The sequence of photos published in *Neue Post* magazine (issue no. 35/97) shows the applicant at the Monte Carlo Beach Club, dressed in a swimsuit and wrapped up in a bathing towel, tripping over an obstacle and falling down. The photos, which are quite blurred, are accompanied by an article entitled "Prince Ernst August played fisticuffs and Princess Caroline fell flat on her face."

[Her initial efforts to secure an injunction against dissemination of the photos failed, prompting a series of appeals.]

23. In a judgment of 19 December 1995, the Federal Court of Justice (*Bundesgerichtshof*) allowed the applicant's appeal in part, granting her an injunction against any further publication of the photos that had appeared in *Freizeit Revue* magazine (issue no. 30 of 22 July 1993) showing her with Vincent Lindon in a restaurant courtyard on the ground that the photos interfered with her right to respect for her private life.

The Federal Court held that even figures of contemporary society "*par excellence*" were entitled to respect for their private life and that this was not limited to their home but also covered the publication of photos. Outside their home, however, they could not rely on the protection of their privacy unless they had retired to a secluded place—away from the public eye—where it was objectively clear to everyone that they wanted to be alone and where, confident of being away from prying eyes, they behaved in a given situation in a manner in which they would not behave in a public place. Unlawful interference with the protection of that privacy could therefore be made out if photos were published that had been taken secretly and/or by catching unawares a person who had retired to such a place. That was the position here, where the applicant and her male companion had withdrawn to the far end of a restaurant courtyard with the clear aim of being out of the public eye.

However, the Federal Court dismissed the remainder of her appeal on the ground that, as a figure of contemporary society "*par excellence,*" the applicant had to tolerate the publication of photos in which she appeared in a public place even if they were photos of scenes from her daily life and not photos showing her exercising her official functions. The public had a legitimate interest in knowing where the applicant was staying and how she behaved in public.

24. The applicant then appealed to the Federal Constitutional Court (*Bundesverfassungsgericht*), submitting that there had been an infringement of her right to the protection of her personality rights.

In the applicant's submission, the criteria established by the Federal Court of Justice regarding the protection of privacy in respect of photos taken in public places did not effectively protect the free development of the personality, be it in the context of private life or family life. Those criteria were so narrow that in practice the applicant could be photographed at any time outside her home and the photos subsequently published in the media.

Given that the photos were not used genuinely to inform people, but merely to entertain them, the right to control the use of one's image in respect of scenes from private life, which had been recognised by the case-law of the Federal Constitutional Court, prevailed over the right—also guaranteed by the Basic Law—to freedom of the press.

25. In a landmark judgment of 15 December 1999, delivered after a hearing, the Constitutional Court allowed the applicant's appeal in part on the ground that the publication of the three photos in issues nos. 32 and 34 of *Bunte* magazine, dated 5 August 1993 and 19 August 1993, featuring the applicant with her children had infringed her right to the protection of her personality rights guaranteed by Articles 2 § 1 and 1 § 1 of the Basic Law, reinforced by her right to family protection under Article 6 of the Basic Law. It referred the case to the Federal Court of Justice on that point. However, the Constitutional Court dismissed the applicant's appeal regarding the other photos.

26. Following the remittal of the case to the Federal Court of Justice in connection with the three photos that had appeared in *Bunte* magazine (issue no. 32 of 5 August 1993 and no. 34 of 19 August 1993) showing the applicant with her children, the Burda publishing company undertook not to republish the photos.

The relevant provisions of the Basic Law [of Germany] are worded as follows:

Article 1 § 1

> "The dignity of human beings is inviolable. All public authorities have a duty to respect and protect it."

Article 2 § 1

> "Everyone shall have the right to the free development of their personality provided that they do not interfere with the rights of others or violate the constitutional order or moral law [*Sittengesetz*]."

Article 5 §§ 1 and 2

> "1. Everyone shall have the right freely to express and disseminate his or her opinions in speech, writing and pictures and freely to obtain information from generally accessible sources. Freedom of the press and freedom of reporting on the radio and in films shall be guaranteed. There shall be no censorship.
>
> 2. These rights shall be subject to the limitations laid down by the provisions of the general laws and by statutory provisions aimed at protecting young people and to the obligation to respect personal honour [*Recht der persönlichen Ehre*]."

Article 6 §§ 1 and 2

> "1. Marriage and the family enjoy the special protection of the State.
>
> 2. The care and upbringing of children is the natural right of parents and a duty primarily incumbent on them. The State community shall oversee the performance of that duty."

The parties' arguments

44. The applicant stated that she had spent more than ten years in unsuccessful litigation in the German courts trying to establish her right to the protection of her private life. She alleged that as soon as she left her house she was constantly hounded by paparazzi who followed her every daily movement, be it crossing the road, fetching her children from school, doing her shopping, out walking, engaging in sport or going on holiday. In her submission, the protection afforded to the private life of a public figure like herself was minimal under German law because the concept of a "secluded place" as defined by the Federal Court of Justice and the Federal Constitutional Court was much too narrow in that respect. Furthermore, in order to benefit from that protection the onus was on her to establish every time that she had been in a secluded place. She was thus deprived of any privacy and could not move about freely without being a target for the paparazzi. She affirmed that in France her prior agreement was necessary for the publication of any photos not showing her at an official event. Such photos were regularly taken in France and then sold and published in Germany. The protection of private life from which she benefited in France was therefore systematically circumvented by virtue of the decisions of the German courts. On the subject of the freedom of the press, the applicant stated that she was aware of the essential role played by the press in a democratic society in terms of informing and forming public opinion, but in her case it was just the entertainment press seeking to satisfy its readers' voyeuristic tendencies and make huge profits from generally innocuous photos showing her going about her daily business. Lastly, the applicant stressed that it was materially impossible to establish in respect of every photo whether or not she had been in a secluded place. As the judicial proceedings were generally held several months after publication of the photos, she was obliged to keep a permanent record of her every movement in order to protect herself from paparazzi who might photograph her. With regard to many of the photos that were the subject of this application, it was impossible to determine the exact time and place at which they had been taken.

45. The Government submitted that German law, while taking account of the fundamental role of the freedom of the press in a democratic society, contained sufficient safeguards to prevent any abuse and ensure the effective protection of the private life of even public figures. In their submission, the German courts had in the instant case struck a fair balance between the applicant's rights to respect for her private life guaranteed by Article 8 and the freedom of the press guaranteed by Article 10, having regard to the margin of appreciation available to the State in this area. The courts had found in the first place that the photos had not been taken in a secluded place and had, subsequently, examined the limits on the protection of private life, particularly in the light of the freedom of the press and even where the publication of photos by the entertainment press was concerned. The protection of the private life of a figure of contemporary society "*par excellence*" did not require the publication of photos without his or her authorisation to be limited to showing the person in question engaged in their official duties. The public had a legitimate interest in knowing how the person behaved generally in public. The Government submitted that this definition of the freedom of the press by the Federal Constitutional Court was compatible with Article 10 and the European Court's relevant case-law. Furthermore, the concept of a secluded place was only one factor, albeit an important one, of which the domestic courts took account when balancing the protection of private life against the freedom of the press. Accordingly, while private life was less well protected where a public figure was photographed in a public place, other factors could also be taken into consideration, such as the nature of the photos, for example, which should not shock the public. Lastly, the Government observed that the decision of the Federal Court of Justice—which had held that the publication of photos of the applicant with the actor Vincent Lindon in a restaurant courtyard in Saint-Rémy-de-Provence were unlawful—showed that the applicant's private life was protected even outside her home.

The Court's assessment

48. The Court notes at the outset that the photos of the applicant with her children are no longer the subject of this application, as it stated in its admissibility decision of 8 July 2003.

The same applies to the photos published in *Freizeit Revue* magazine (issue no. 30 of 22 July 1993) showing the applicant with Vincent Lindon at the far end of a restaurant courtyard in Saint-Rémy-de-Provence. In its judgment of 19 December 1995, the Federal Court of Justice prohibited any further publication of the photos on the ground that they infringed the applicant's right to respect for her private life.

Applicability of Article 8 [of the European Convention of Human Rights]

50. The Court reiterates that the concept of private life extends to aspects relating to personal identity, such as a person's name or a person's picture.

Furthermore, private life, in the Court's view, includes a person's physical and psychological integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings. There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life."

51. The Court has also indicated that, in certain circumstances, a person has a "legitimate expectation" of protection and respect for his or her private life. Accordingly, it has held in a case concerning the interception of telephone calls on business premises that the applicant "would have had a reasonable expectation of privacy for such calls."

52. As regards photos, with a view to defining the scope of the protection afforded by Article 8 against arbitrary interference by public authorities, the European Commission of Human Rights had regard to whether the photographs related to private or public matters and whether the material thus obtained was envisaged for a limited use or was likely to be made available to the general public.

53. In the present case there is no doubt that the publication by various German magazines of photos of the applicant in her daily life either on her own or with other people falls within the scope of her private life.

Compliance with Article 8

54. In the present case the applicant did not complain of an action by the State, but rather of the lack of adequate State protection of her private life and her image.

57. The Court reiterates that, although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. That also applies to the protection of a person's picture against abuse by others.

The boundary between the State's positive and negative obligations under this provision does not lend itself to precise definition. The applicable principles are, nonetheless, similar. In both contexts regard must be had to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole; and in both contexts the State enjoys a certain margin of appreciation.

58. That protection of private life has to be balanced against the freedom of expression guaranteed by Article 10 of the Convention.

In that context, the Court reiterates that freedom of expression constitutes one of the essential foundations of a democratic society. Subject to paragraph 2 of Article 10, it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society."

In that connection, the press plays an essential role in a democratic society. Although it must not overstep certain bounds, in particular in respect of the reputation and rights of others, its duty is nevertheless to impart—in a manner consistent with its obligations and responsibilities—information and ideas on all matters of public interest. Journalistic freedom also covers possible recourse to a degree of exaggeration, or even provocation.

59. Although freedom of expression also extends to the publication of photos, this is an area in which the protection of the rights and reputation of others takes on particular importance. The present case does not concern the dissemination of "ideas," but of images containing very personal or even intimate "information" about an individual. Furthermore, photos appearing in the tabloid press are often taken in a climate of continual harassment which induces in the person concerned a very strong sense of intrusion into their private life or even of persecution.

60. In the cases in which the Court has had to balance the protection of private life against freedom of expression, it has always stressed the contribution made by photos or articles in the press to a debate of general interest. The Court thus found, in one case, that the use of certain terms in relation to an individual's private life was not "justified by considerations of public concern" and that those terms did not "[bear] on a matter of general importance" and went on to hold that there had not been a violation of Article 10. In another case, however, the Court attached particular importance to the fact that the subject in question was a news item of "major public concern" and that the published photographs "did not disclose any details of [the] private life" of the person in question and held that there had been a violation of Article 10. Similarly, in a recent case concerning the publication by President Mitterrand's former private doctor of a book containing revelations about the President's state of health, the Court held that "the more time that elapsed, the more the public interest in discussion of the history of President Mitterrand's two terms of office prevailed over the requirements of protecting the President's rights with regard to medical confidentiality" and held that there had been a breach of Article 10.

61. The Court notes at the outset that in the present case the photos of the applicant in the various German magazines show her in scenes from her daily life, thus involving activities of a purely private nature such as engaging in sport, out walking, leaving a restaurant or on holiday. The photos, in which the applicant appears sometimes alone and sometimes in company, illustrate a series of articles with such innocuous titles as "Pure happiness," "Caroline . . . a woman returning to life," "Out and about with Princess Caroline in Paris," and "The kiss. Or: they are not hiding anymore."

62. The Court also notes that the applicant, as a member of the Prince of Monaco's family, represents the ruling family at certain cultural or charitable events. However, she does not exercise any function within or on behalf of the State of Monaco or any of its institutions (see paragraph 8 above).

63. The Court considers that a fundamental distinction needs to be made between reporting facts—even controversial ones—capable of contributing to a debate in a democratic society relating to politicians in the exercise of their functions, for example, and reporting details of the private life of an individual who, moreover, as in this case, does not exercise official functions. While in the former case the press exercises its vital role of "watchdog" in a democracy

by contributing to "impart[ing] information and ideas on matters of public interest," it does not do so in the latter case.

64. Similarly, although the public has a right to be informed, which is an essential right in a democratic society that, in certain special circumstances, can even extend to aspects of the private life of public figures, particularly where politicians are concerned, this is not the case here. The situation here does not come within the sphere of any political or public debate because the published photos and accompanying commentaries relate exclusively to details of the applicant's private life.

65. As in other similar cases it has examined, the Court considers that the publication of the photos and articles in question, the sole purpose of which was to satisfy the curiosity of a particular readership regarding the details of the applicant's private life, cannot be deemed to contribute to any debate of general interest to society despite the applicant being known to the public.

66. In these conditions freedom of expression calls for a narrower interpretation.

67. In that connection, the Court also takes account of the resolution of the Parliamentary Assembly of the Council of Europe on the right to privacy, which stresses the "one-sided interpretation of the right to freedom of expression" by certain media which attempt to justify an infringement of the rights protected by Article 8 of the Convention by claiming that "their readers are entitled to know everything about public figures."

68. The Court finds another point to be of importance: even though, strictly speaking, the present application concerns only the publication of the photos and articles by various German magazines, the context in which these photos were taken—without the applicant's knowledge or consent—and the harassment endured by many public figures in their daily lives cannot be fully disregarded.

In the present case this point is illustrated in particularly striking fashion by the photos taken of the applicant at the Monte Carlo Beach Club tripping over an obstacle and falling down. It appears that these photos were taken secretly at a distance of several hundred metres, probably from a neighbouring house, whereas journalists' and photographers' access to the club was strictly regulated.

69. The Court reiterates the fundamental importance of protecting private life from the point of view of the development of every human being's personality. That protection—as stated above—extends beyond the private family circle and also includes a social dimension. The Court considers that anyone, even if they are known to the general public, must be able to enjoy a "legitimate expectation" of protection of and respect for their private life.

70. Furthermore, increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data. This also applies to the systematic taking of specific photos and their dissemination to a broad section of the public.

74. The Court therefore considers that the criteria on which the domestic courts based their decisions were not sufficient to protect the applicant's private life effectively. As a figure of contemporary society "*par excellence*" she cannot—in the name of freedom of the press and the public interest—rely on protection of her private life unless she is in a secluded place out of the public eye and, moreover, succeeds in proving it (which can be difficult). Where that is not the case, she has to accept that she might be photographed at almost any time, systematically, and that the photos are then very widely disseminated even if, as was the case here, the photos and accompanying articles relate exclusively to details of her private life.

75. In the Court's view, the criterion of spatial isolation, although apposite in theory, is in reality too vague and difficult for the person concerned to determine in advance. In the

present case, merely classifying the applicant as a figure of contemporary society "*par excellence*" does not suffice to justify such an intrusion into her private life.

76. As the Court has stated above, it considers that the decisive factor in balancing the protection of private life against freedom of expression should lie in the contribution that the published photos and articles make to a debate of general interest. It is clear in the instant case that they made no such contribution, since the applicant exercises no official function and the photos and articles related exclusively to details of her private life.

77. Furthermore, the Court considers that the public does not have a legitimate interest in knowing where the applicant is and how she behaves generally in her private life even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public.

Even if such a public interest exists, as does a commercial interest of the magazines in publishing these photos and these articles, in the instant case those interests must, in the Court's view, yield to the applicant's right to the effective protection of her private life.

78. Lastly, in the Court's opinion the criteria established by the domestic courts were not sufficient to ensure the effective protection of the applicant's private life and she should, in the circumstances of the case, have had a "legitimate expectation" of protection of her private life.

79. Having regard to all the foregoing factors, and despite the margin of appreciation afforded to the State in this area, the Court considers that the German courts did not strike a fair balance between the competing interests.

80. There has therefore been a breach of Article 8 of the Convention

Notes

1. What is the fundamental difference between privacy as understood by the European Court of Human Rights (ECHR) and privacy as understood by the German courts? Is it as simple as the German courts taking an American-like perspective that "if in public, then not private" and the ECHR disagreeing? Do the German courts think that more is private than would a similarly situated American court? One is tempted to create a spectrum. The ECHR treating a range of everyday activities that occur in public places as still private, provided there is no newsworthy value; the German courts requiring people to retreat into at least some degree of physical seclusion for them to receive privacy protection (or to have photos involving children); and Americans requiring something truly exceptional to credit a privacy claim in a public place. But this is likely a gross oversimplification.
2. Princess Caroline brought two subsequent cases to the ECHR, *Von Hannover v. Germany No. 2* (2012) and *Von Hannover v. Germany, No. 3* (2013), and lost both. *Von Hannover No. 3* is only available in French, but the court provided this English language summary:

> The photograph at issue in the present application was published in the magazine 7 Tage on 20 March 2002. It showed the applicant and her husband on holiday in an unidentifiable location. On the same page and the following page were several photographs of the von Hannover holiday home situated on an island off Kenya. The photographs were accompanied by an article stating that it had become the custom among celebrities to let out their holiday homes. The article went on to describe the von Hannover family's villa, giving details of the furnishings, the daily rental cost and different holiday pastimes. A small box inserted in the text contained two sentences in bold type which read: "The rich and beautiful are also thrifty ("sparsam"). Many of them let out their villas to paying guests."

> In its judgments in *Axel Springer AG* and *Von Hannover (no. 2)* the Court had set forth the relevant criteria for balancing the right to respect for private life against the right to freedom of expression. These were: contribution to a debate of general interest, how well known the person concerned was, the subject of the report, the prior conduct of the person concerned, the content, form and consequences of the publication and, in the case of photographs, the circumstances in which they were taken.
>
> The Court noted that in the present application the Federal Constitutional Court had taken the view that, while the photograph in question had not contributed to a debate of general interest, the same was not true of the article accompanying it, which reported on the current trend among celebrities towards letting out their holiday homes. The Federal Constitutional Court and, subsequently, the Federal Court of Justice had observed that the article was designed to report on that trend and that this conduct was apt to contribute to a debate of general interest. The Court also noted that the article itself did not contain information concerning the private life of the applicant or her husband, but focused on practical aspects relating to the villa and its letting.
>
> It could not therefore be asserted that the article had merely been a pretext for publishing the photograph in question or that the connection between the article and the photograph had been purely contrived. The characterisation of the subject of the article as an event of general interest, first by the Federal Constitutional Court and then by the Federal Court of Justice, could not be considered unreasonable. The Court could therefore accept that the photograph in question had made a contribution to a debate of general interest.
>
> As to how well known the applicant was, the Court pointed out that it had found on several occasions that the applicant and her husband were to be regarded as public figures who could not claim protection of their private lives in the same way as individuals unknown to the public.
>
> Noting that the German courts had taken into consideration the essential criteria and the Court's case-law in balancing the various interests at stake, the Court concluded that they had not failed to comply with their positive obligations and that there had been no violation of Article 8 of the Convention.[251]

In addition to this summary of the overall doctrine, consider this excerpt from *Von Hannover No. 2*, on newsworthiness:

> An initial essential criterion is the contribution made by photos or articles in the press to a debate of general interest. The definition of what constitutes a subject of general interest will depend on the circumstances of the case. The Court nevertheless considers it useful to point out that it has recognised the existence of such an interest not only where the publication concerned political issues or crimes, but also where it concerned sporting issues or performing artists. However, the rumoured marital difficulties of the President of a country or the financial difficulties of a famous singer were not deemed to be matters of general interest.

Does this appear to mark a retreat from *Von Hannover No. 1*? The doctrine of newsworthiness endorsed here seems broader than one might have expected, as the renting of summer homes is hardly a matter of key political interest, and the photo in question adds

---

[251] Available at https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-4498929-5425601%22]}.

little to the story. Yet there are still limitations. The article does not appear to have been a mere excuse for the photo here, whereas the photos in *Von Hannover No. 1* appear to have been the sole point of the stories. Also, the marital problems of a major political or business leader likely would be newsworthy by American standards, but are not under these rules.

B. The Data Protection Directive and the Right to be Forgotten

In addition to these constitutional-style provisions from the Council of Europe, European privacy law also has major statutory frameworks through the European Union. Previously, the primary framework was the Data Protection Directive of 1995 (95/46/EC). Though this Directive was critical to understand prior to 2018, it has since been supplanted. It is mentioned here for two reasons. First, to explain the difference between a "directive" and a "regulation" in EU law. Directives are fundamentally addressed to the member states, requiring them to pass implementing legislation to achieve certain goals but allowing for a degree of flexibility in how those goals are reached. This creates a certain amount of heterogeneity. Regulations, by contrast, are self-executing laws. Member states are involved in enforcing these laws, but the law itself is uniform throughout the EU. This is part of why it was such a major event when the European Parliament and the Council of the European Union adopted the General Data Protection Regulation 2016/679 (GDPR), which took effect in 2018. GDPR is the law throughout the EU and has been a model for legislation in a number of other countries.[252]

The second reason the Directive is mentioned is because some of the key cases under the Directive inform European privacy law even after the implementation of GDPR. Among the best-known of these cases is *Google Spain*, which is credited for creating the "Right to be Forgotten." As you read it, think about how American law would deal with this type of claim.

Google Spain SL v. Agencia Española de Protección de Datos (AEPD), No. C-131/12, E.C.J. (2014)

1. This request for a preliminary ruling concerns the interpretation of Article 2(b) and (d), Article 4(1)(a) and (c), Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) and of Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

14. On 5 March 2010, Mr. Costeja González, a Spanish national resident in Spain, lodged with the AEPD a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, in particular in Catalonia (Spain) ('La Vanguardia'), and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered Mr. Costeja González's name in the search engine of the Google group ('Google Search'), he would obtain links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr. Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

15. By that complaint, Mr. Costeja González requested, first, that La Vanguardia be required either to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the

[252] After leaving the EU, the United Kingdom enacted its own data protection statute that is identical to GDPR.

data. Second, he requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to La Vanguardia. Mr. Costeja González stated in this context that the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant.

16. By decision of 30 July 2010, the AEPD rejected the complaint in so far as it related to La Vanguardia, taking the view that the publication by it of the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible.

17. On the other hand, the complaint was upheld in so far as it was directed against Google Spain and Google Inc. The AEPD considered in this regard that operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society. The AEPD took the view that it has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties. The AEPD considered that that obligation may be owed directly by operators of search engines, without it being necessary to erase the data or information from the website where they appear, including when retention of the information on that site is justified by a statutory provision.

18. Google Spain and Google Inc. brought separate actions against that decision before the Audiencia Nacional (National High Court) [,which referred key questions to this court.]

[Do search engines process personal data within the meaning of the Directive?]

25. Article 2(b) of Directive 95/46 defines 'processing of personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.'

26. As regards in particular the internet, the Court has already had occasion to state that the operation of loading personal data on an internet page must be considered to be such 'processing' within the meaning of Article 2(b) of Directive 95/46.

27. So far as concerns the activity at issue in the main proceedings, it is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons and thus 'personal data' within the meaning of Article 2(a) of that directive.

28. Therefore, it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves,' 'records,' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data.

29. Nor is the foregoing finding affected by the fact that those data have already been published on the internet and are not altered by the search engine.

32. As to the question whether the operator of a search engine must be regarded as the 'controller' in respect of the processing of personal data that is carried out by that engine in the context of an activity such as that at issue in the main proceedings, it should be recalled that Article 2(d) of Directive 95/46 defines 'controller' as 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.'

33. It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d).

34. Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective—which is to ensure, through a broad definition of the concept of 'controller,' effective and complete protection of data subjects—to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.

36. Moreover, it is undisputed that that activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published.

39. Finally, the fact that publishers of websites have the option of indicating to operators of search engines, by means in particular of exclusion protocols such as 'robot.txt' or codes such as 'noindex' or 'noarchive', that they wish specific information published on their site to be wholly or partially excluded from the search engines' automatic indexes does not mean that, if publishers of websites do not so indicate, the operator of a search engine is released from its responsibility for the processing of personal data that it carries out in the context of the engine's activity.

41. It follows from all the foregoing considerations that . . . the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' . . . and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).

[Is Google within the territorial scope of the Directive?]

43. In this respect, the referring court has established the following facts:

— Google Search is offered worldwide through the website 'www.google.com.' In numerous States, a local version adapted to the national language exists. The version of Google Search in Spanish is offered through the website 'www.google.es', which has been registered since 16 September 2003. Google Search is one of the most used search engines in Spain.

— Google Search indexes websites throughout the world, including websites located in Spain. The information indexed by its 'web crawlers' or robots, that is to say, computer programmes used to locate and sweep up the content of web pages methodically and automatically, is stored temporarily on servers whose State of location is unknown, that being kept secret for reasons of competition.

— Google Search does not merely give access to content hosted on the indexed websites, but takes advantage of that activity and includes, in return for payment, advertising associated with the internet users' search terms, for

undertakings which wish to use that tool in order to offer their goods or services to the internet users.

— The Google group has recourse to its subsidiary Google Spain for promoting the sale of advertising space generated on the website 'www.google.com.' Google Spain, which was established on 3 September 2003 and possesses separate legal personality, has its seat in Madrid (Spain).

— Google Inc. designated Google Spain as the controller, in Spain, in respect of two filing systems registered by Google Inc. with the AEPD; those filing systems were intended to contain the personal data of the customers who had concluded contracts for advertising services with Google Inc.

44. Specifically, the main issues raised by the referring court concern the notion of 'establishment,' within the meaning of Article 4(1)(a) of Directive 95/46, and of 'use of equipment situated on the territory of the said Member State,' within the meaning of Article 4(1)(c).

55. In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.

56. In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.

57. As has been stated in paragraphs 26 to 28 of the present judgment, the very display of personal data on a search results page constitutes processing of such data. Since that display of results is accompanied, on the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory.

58. That being so, it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46 . . . .

[Do search engines ever have to take down links to content lawfully posted online?]

80. It must be pointed out at the outset that processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet—information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty—and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous.

81. In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing. However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

84. Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites.

85. Furthermore, the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' and thus benefit, by virtue of Article 9 of Directive 95/46, from derogations from the requirements laid down by the directive, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine. It cannot therefore be ruled out that in certain circumstances the data subject is capable of exercising the rights referred to in Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 against that operator but not against the publisher of the web page.

86. Finally, it must be stated that not only does the ground, under Article 7 of Directive 95/46, justifying the publication of a piece of personal data on a website not necessarily coincide with that which is applicable to the activity of search engines, but also, even where that is the case, the outcome of the weighing of the interests at issue to be carried out under Article 7(f) and subparagraph (a) of the first paragraph of Article 14 of the directive may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of the web page is at issue, given that, first, the legitimate interests justifying the processing may be different and, second, the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same.

87. Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person's name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page.

88. In the light of all the foregoing considerations . . . Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

[Should links to this information be taken down?]

89. [T]he referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as enabling the data subject to require the operator of a search engine to remove from the list of results displayed following a search made on the basis of his name links to web pages published lawfully by third parties and containing true information relating to him, on the ground that that information may be prejudicial to him or that he wishes it to be 'forgotten' after a certain time.

92. As regards Article 12(b) of Directive 95/46, the application of which is subject to the condition that the processing of personal data be incompatible with the directive, such incompatibility may result not only from the fact that such data are inaccurate but, in particular, also from the fact that they are inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes.

93. It follows from those requirements, laid down in Article 6(1)(c) to (e) of Directive 95/46, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.

94. Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.

96. In the light of the foregoing, when appraising such requests made in order to oppose processing such as that at issue in the main proceedings, it should in particular be examined whether the data subject has a right that the information relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name. In this connection, it must be pointed out that it is not necessary in order to find such a right that the inclusion of the information in question in the list of results causes prejudice to the data subject.

97. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held, as follows in particular from paragraph 81 of the present judgment, that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.

98. As regards a situation such as that at issue in the main proceedings, which concerns the display, in the list of results that the internet user obtains by making a search by means of Google Search on the basis of the data subject's name, of links to pages of the on-line archives of a daily newspaper that contain announcements mentioning the data subject's name and

relating to a real-estate auction connected with attachment proceedings for the recovery of social security debts, it should be held that, having regard to the sensitivity for the data subject's private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list. Accordingly, since in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information, a matter which is, however, for the referring court to establish, the data subject may, by virtue of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, require those links to be removed from the list of results.

Notes

1. Under American law, this would be unconstitutional. Information in public records is not private (*Cox Broadcasting*, *Florida Star*) and republisher immunity is a defense to public disclosure of private facts. So, there could never be liability for linking to someone else's truthful post about a person merely on the grounds that the information in that post is no longer relevant.
2. In terms of policy, is *Google Spain* reaching a good result? Is it better to live in a place where old press coverage and announcements about people are readily searchable online, or better to live in a place where they may not be? Should people be able to "memory hole" their college antics? How relevant is decades-old information about minor activities, or even minor crimes, to online strangers?
   Choose a few current or former classmates and run online searches about them. You may find highly relevant information, but you will also find what is effectively useless garbage. Sports results from their time on their college rowing team. Quotes from their campus newspaper. An award they won in high school. One of my friends in college was the contact person for several campus clubs. For over a decade after graduation, his old college event postings were high in his search results. His political and religious beliefs evolved substantially after graduation, making these older results rather awkward. Should he have had the legal ability to get them removed? Is there social benefit to keeping them in place?
3. Between May 2014 and September 2024, Google received over 1.6 million requests to delist content, targeting over 6.4 million URLs.[253] In the first half of 2024, approximately 60 percent of URL delist requests were granted. According to Google, its evaluation process for such requests consists of four steps:

   > 1. Does the request contain all the necessary information for us to be able to make a decision?
   >
   > 2. Does the person making the request have a connection to a European country, such as residency or citizenship?
   >
   > 3. Do the pages appear in search results for the requester's name and does the requester's name appear on the page(s) requested for delisting?
   >
   > 4. Does the page requested for delisting include information that is inadequate, irrelevant, no longer relevant, or excessive, based on the information that the requester provides? Is there a public interest in that information remaining available in search results generated by a search for the requester's name?[254]

---

[253] *Requests to delist under European privacy law*, GOOGLE TRANSPARENCY REPORT, https://transparencyreport.google.com/eu-privacy/overview.

[254] *European privacy requests Search removals FAQs*, TRANSPARENCY REPORT HELP CENTER, https://support.google.com/transparencyreport/answer/7347822#requester&zippy=%2Chow-do-you-evaluate-requests.

Of these, the fourth is obviously the most substantive, asking for the kind of balancing analysis contemplated by *Google Spain*. When requests are denied, the requester can appeal to their country's Data Protection Authority.

4. Google further publishes a list of selected decisions that it has made.[255] These are from 2022 and are organized by country.

Belgium

Request 1

> Request: We received a request from an individual to delist 4 URLs: 2 news articles from 2007 and 2 archived documents from the 1980s, including one hosted on a government website. The URLs discussed important historical events which had taken place in a country in South America and in which the individual had been involved. The request stated that the URLs presented a risk to both the physical and psychological stability of the individual and of their family.
>
> Outcome: We did not delist any of the URLs in light of the historical nature of the events and involvement of the requestor.

Request 2

> Request: We received a request from a social worker to delist 5 news articles on behalf of an individual. The articles stated that the individual had been found guilty of multiple accounts of rape and sexual abuse against a family member and two other underaged victims; they received a 7-year prison sentence in 2006.
>
> Outcome: We did not delist 4 URLs requested given the severity of the crime, the sentence they received, and the time that had passed since the sentence had ended. We asked the individual for more information regarding the remaining URL.

Denmark

> Request: We received a request from an individual to delist 2 URLs published in 2001 on news websites. The articles reported on the 6-year prison sentence imposed on the individual for their involvement in a fatal shooting incident which had taken place in 2001.
>
> Outcome: We delisted 1 URL given the time that had passed since the individual's sentence had ended. We asked the individual for more information regarding the remaining URL.

France

Request 1

> Request: We received a request from a well-known actress to delist 1 news article, published in 2012, which reported on an incident involving the actress and which had taken place in a public setting.
>
> Outcome: We delisted the URL given the private nature of the incident, not related to the individual's work or role in public life, and because of the time that had passed since the publication.

Request 2

> Request: We received a request from the French Data Protection Authority, made on behalf of a former politician turned teacher, to delist 4 URLs (2 news articles

[255] *Requests to delist content under European privacy law*, *supra* note 253.

from 2013, 1 YouTube video and 1 blog post). The content at issue described how the individual, who had been a candidate in a local election, was evicted from his political party for extremist views. Following his eviction, the individual had left politics and is now a teacher. The DPA argued that the content should be delisted given that it was old and the individual, having withdrawn from political life, was no longer a public person.

Outcome: We agreed to delist all 4 URLs.

Request 3

Request: We received a binding order from the French Data Protection Authority, made on behalf of a former politician, to delist 3 blog posts dated 2014 which made reference to the individual's local election campaign. The DPA ordered the delisting on the basis that the individual is not a public person given that they no longer have a political mandate and achieved barely 1% of votes in the last local elections.

Outcome: We delisted all 3 URLs subject to the DPA's order.

Luxembourg

Request: We received a request from a finance professional to delist 1 URL, a news article published in 2015. The article reported allegations of money laundering and of fraud with regard to a real estate deal. The requestor provided judicial documentation which demonstrated that they had been cleared of the money laundering accusations.

Outcome: We did not delist the URL. While the money laundering accusations had been dismissed, there was no indication that the fraud accusations had been, and they continued to appear relevant based on information available to us.

Netherlands

Request: We received a request to delist 6 URLs, published in 2018 and 2019, reporting on the requestor's participation in a volunteer project with local children.

Outcome: We delisted 3 of the URLs as they relate to volunteer projects that did not seem to form a part of the individual's role in public life. We delisted 2 of the URLs as we could not locate the individual's name on the webpages. We did not delist the remaining URL as it was not in the Google Search index.

Norway

Request: We received a request from a property agent to delist 7 URLs: 4 were news articles published between 2009 and 2016 and 3 were hosted on aggregator websites. The URLs reported on the individual's 5-year conviction for fraud in their professional capacity.

Outcome: We did not delist 6 of the URLs as the conviction remains of relevance to the requester's professional life and therefore of interest to the public. We did not delist the remaining URL because the page was blocked and we could not access it

United Kingdom

Request 1

Request: We received a request from an individual to delist 8 URLs related to their career as a singer-songwriter. The individual argued that the URLs should be delisted because they had changed profession in 2019 to become a journalist.

Outcome: We delisted 2 URLs as the content had been removed at the source by the webmaster. We did not delist the remaining 6 URLs given the recency of the career change and therefore the potential to re-enter that field.

Request 2

Request: We received a request to delist 1 URL published in 2020 on a news site and which listed all individuals convicted that week at the regional tribunal. The requester had been convicted to a 16-week jail term (suspended for 12 months) and banned from driving for 36 months, for driving under the influence of alcohol and without insurance.

Outcome: We delisted the URL as the requestor's jail conviction was spent.

Note several themes. First, people who have withdrawn from public life are allowed to remove evidence of their past activities, even if those activities were then in the public eye (France Requests 2 and 3). People who had criminal convictions may be able to remove links to them (Denmark; United Kingdom Request 2), but not if the crimes are recent, especially serious, or otherwise continually relevant (Belgium Request 2; Luxembourg; Norway). Cases with apparently de minimis public interest in keeping the information available (France Request 1; Netherlands) seem to have been easy for Google to grant.

C. Basic Features of the General Data Protection Regulation

Enacted in 2016, the General Data Protection Regulation (GDPR) went into effect on May 25, 2018. It replaced the Data Protection Directive of 1995, substantially raised privacy standards throughout Europe and established a greater degree of uniformity in privacy enforcement.

Material Scope. GDPR applies to the processing of personal data "by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." Article 2.1. It does not apply to processing by "a natural person in the course of a purely personal or household activity" or to the processing of personal data by "competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences." Article 2.2.

Territorial Scope. GDPR applies to data controllers and processors operating within the EU—even if they are processing non-EU data—as well as those outside the EU that offer goods or services to, or monitor the behavior of, EU residents. Article 3. This extraterritorial application is crucial, making GDPR relevant to businesses worldwide, including American companies that engage with European customers or manage European workers. When a foreign website is available in the EU but does not target EU consumers—for instance, does not offer delivery to Europe or list prices in Euros – it will generally not fall within the scope of GDPR even if occasionally users are EU residents.

Personal Data. Personal data is defined broadly. It "means any information relating to an identified or identifiable natural person." Further, "an identifiable natural person is one who can be identified, directly or indirectly." Article 4.1. Online identifiers such as IP addresses count as identifiable.

Controllers and Processors. GDPR places responsibilities on two types of entities: controllers and processors. A data controller "determines the purposes and means of processing personal data." Article 4.7. A data processor acts on behalf of the controller and processes the data according to the controller's instructions. Article 4.8. A given set of data may be subject to

multiple or joint controllers. Article 26. The controller has the primary obligation for ensuring compliance with GDPR. Article 24. Processors must abide by their processing agreements with the controller (meaning not process the data for their own purposes as well), not engage sub-processors without the controller's authorization, and ensure the security of all data. Article 28.

Principles. Article 5 sets out the main principles related to the processing of personal data under GDPR. According to it:

> Personal data shall be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes [except for permitted scientific and historical research under Article 89] ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation');
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

GDPR assumes that data processors and controllers should not collect all possible data (minimization), should collect data only for defined purposes (purpose limitation), and should process that data lawfully, fairly, and transparently. Consider the contrast between this set of assumptions and the approach of a traditional American technology company in the early 2000s. The American approach was generally to collect all possible information on consumers and figure out what economic value could be wrung from it afterwards. It is only with the advent of state consumer privacy laws and a somewhat more energized FTC in the late 2010s and early 2020s that the American model began to change.

The American privacy lawyer should be reminded of HIPAA as they read through these provisions. In particular, the emphasis on data minimization and the need to take care when processing identifiable (and not just identified) data appears in both statutes. But HIPAA is arguably the strongest sectoral American statute and applies only to a narrow subset of data whereas GDPR applies to all data processing in the EU. Also, the requirement that data be kept up to date and deleted when no longer needed is related to the right to be forgotten and *Google Spain* case; GDPR continues the regulatory threads that began in the Data Protection Directive. The "right to erasure" is further addressed in Article 17.

Lawful Processing. GDPR goes on to define "lawful" processing in Article 6:

> Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Points (a) and (b) are the most critical. To process personal data in the EU, a data controller must either have the consent of the data subject or be processing in response to the request of the data subject. Further**, c**onsent must be "freely given, specific, informed and unambiguous." It requires either "a statement or . . . a clear affirmative action." Article 4.11. Consent should be as easy to withdraw as it is to grant and requests for consent should be presented in clear and plain language. Article 7.

For consent to be informed and specific, the data subject must at least be notified about the controller's identity, what kind of data will be processed, how it will be used and the purpose of the processing operations as a safeguard against "function creep." This consent must be specific rather than general.[256] The data subject must also be informed about his or her right to withdraw consent anytime. Where relevant, the controller also has to inform the data subject about the use of the data for automated decision-making and the possible risks of data transfers due to absence of an adequacy decision or other appropriate safeguards.

For consent to be "freely given" there must be "real choice and control."[257] "As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid." Further, "[i]f consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given."[258]

Even when data is being lawfully processed, GDPR grants the data subject a series of key rights.

1. **Right of access**. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data. Further, the controller must provide to the data subject information about the purpose of the processing, the categories of data processed, the duration of storage, and the identities of any third parties who will have access to the data. Article 15.
2. **Right to rectification.** The data subject shall have the right to obtain from the controller without undue delay the correction of inaccurate personal data concerning

---

[256] European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679 ¶ 55 (May 4, 2020), https://edpb.europa.eu/our-work-tools/ourdocuments/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[257] *Id.* at ¶ 13.

[258] *Id.*

him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed. Article 16.

3. **Right to erasure.** The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data when:
    a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
    b. the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing; or
    c. the personal data have been unlawfully processed.

    But a controller need not delete the data if the processing is necessary for exercising the right of freedom of expression and information. Article 17.
4. **Right to restrict processing.** The controller must restrict processing of information when the accuracy is contested and the controller is verifying the accuracy, when the data is no longer needed for their original purpose but the data must be retained for legal reasons, or when the data subject has exercised their right to object. Article 18.
5. **Right to data portability**. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller. Article 20.
6. **Right to object**. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6, the provisions that allow for the lawful processing of data based on the legitimate interests of the controller or in the public interest. If the objection is made, the controller must demonstrate that the relevant provision applies. Further, the data subject can object to the use of their data for direct marketing, and the controller must cease such use upon objection. Article 21.

Special categories of personal data. Certain data is defined as sensitive data under GDPR. Specifically: "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." Article 9. Sensitive personal data can only be processed if the controller can show that one of a list of defined exceptions applies. The first and likely most relevant of these exceptions is "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes." Other exceptions include: "processing relates to personal data which are manifestly made public by the data subject;" and "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

Data Protection Officer. A Data Protection Officer (DPO) is an employee within an organization who is responsible for understanding the GDPR and ensuring the organization's compliance. The DPO is the main point of contact for the data protection authority. Typically, the DPO has knowledge of both information technology and law.

Enforcement and penalties. The GDPR allows the national data protection authorities in each country to issue sanctions and fines to organizations it finds in violation. The maximum penalty is twenty million euros or four percent of global revenue, whichever is higher. Data protection authorities can also issue sanctions, such as bans on data processing or public reprimands.

The below *Planet49* case is primarily about GDPR. Because Planet49's conduct overlapped with the date of GDPR implementation, however, there is also discussion of the earlier laws. Notably:

- Directive 95/46: The Data Protection Directive (which was directly replaced by GDPR)
- Directive 2002/58: The ePrivacy Directive

EU decisions often refer to these directives by number rather than by name. They also often refer to GDPR as Regulation 2016/679.

Consider this language from the ePrivacy Directive, Article 5(3):

> "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."

This is a requirement to get consent to install "cookies" on a user's computer except as necessary to perform the services requested by the user. The meaning of consent under the ePrivacy Directive, informed by the later GDPR, is the main issue in the *Planet49* case.

Bundesverband der Verbraucherzentralen und Verbraucherverbände v. Planet49 GmbH, No. C-673/17, E.C.J. (2019)

25. On 24 September 2013, Planet49 organised a promotional lottery on the website www.dein-macbook.de.

26. Internet users wishing to take part in that lottery were required to enter their postcodes, which redirected them to a web page where they were required to enter their names and addresses. Beneath the input fields for the address were two bodies of explanatory text accompanied by checkboxes. The first body of text with a checkbox without a preselected tick ('the first checkbox') read:

> 'I agree to certain *sponsors and cooperation partners* providing me with information by post or by telephone or by email/SMS about offers from their *respective commercial sectors*. I can determine these myself here; otherwise, the selection is made by the organiser. I can revoke this consent at any time. *Further information about this can be found here*.'

27. The second set of text with a checkbox containing a preselected tick ('the second checkbox') read:

> 'I agree to the web analytics service Remintrex being used for me. This has the consequence that, following registration for the lottery, the lottery organiser, [Planet49], sets cookies, which enables Planet49 to evaluate my surfing and use behaviour on websites of advertising partners and thus enables advertising by Remintrex that is based on my interests. I can delete the cookies at any time. You can read more about this *here*.'

28. Participation in the lottery was possible only if at least the first checkbox was ticked.

29. The hyperlink associated with the words 'sponsors and cooperation partners' and 'here' next to the first checkbox opened a list of 57 companies, their addresses, the commercial sector to be advertised and the method of communication used for the advertising (email, post or telephone). The underlined word 'Unsubscribe' was contained after the name of each company. The following statement preceded the list:

> 'By clicking on the "Unsubscribe" link, I am deciding that no advertising consent is permitted to be granted to the partner/sponsor in question. If I have not unsubscribed from any or a sufficient number of partners/sponsors, Planet49 will choose partners/sponsors for me at its discretion (maximum number: 30 partners/sponsors).'

30. When the hyperlink associated with the word 'here' next to the second checkbox was clicked on, the following information was displayed:

> 'The cookies . . . are small files which are stored in an assigned manner on your hard disk by the browser you use and by means of which certain information is supplied which enables more user-friendly and effective advertising. The cookies contain a specific randomly generated number (ID), which is at the same time assigned to your registration data. If you then visit the website of an advertising partner which is registered for Remintrex (to find out whether a registration exists, please consult the advertising partner's data protection declaration), Remintrex automatically records, by virtue of an iFrame which is integrated there, that you (or the user with the stored ID) have visited the site, which product you have shown interest in and whether a transaction was entered into.
>
> Subsequently, [Planet49] can arrange, on the basis of the advertising consent given during registration for the lottery, for advertising emails to be sent to you which take account of your interests demonstrated on the advertising partner's website. After revoking the advertising consent, you will of course not receive any more email advertising.
>
> The information communicated by these cookies is used exclusively for the purposes of advertising in which products of the advertising partner are presented. The information is collected, stored and used separately for each advertising partner. User profiles involving multiple advertising partners will not be created under any circumstances. The individual advertising partners do not receive any personal data.
>
> If you have no further interest in using the cookies, you can delete them via your browser at any time. You can find a guide in your browser's ["help"] function.
>
> No programs can be run or viruses transmitted by means of the cookies.
>
> You of course have the option to revoke this consent at any time. You can send the revocation in writing to [Planet49] [address]. However, an email to our customer services department [email address] will also suffice.'

31. According to the order for reference, cookies are text files which the provider of a website stores on the website user's computer which that website provider can access again when the user visits the website on a further occasion, in order to facilitate navigation on the internet or transactions, or to access information about user behaviour.

Consideration of the questions referred

Preliminary observations

41. [I]n view of the entry into force, on 25 May 2018, of Regulation 2016/679 [GDPR], . . . it was likely that that regulation would need to be taken into account when disposing of the

case in the main proceedings. In addition, as the German Government stated at the hearing before the Court, it is not inconceivable that, in so far as the proceedings brought by the Federation seek an order that Planet49 refrain from future action, Regulation 2016/679 would be applicable *ratione temporis* to the case in the main proceedings . . . .

43. The questions referred must therefore be answered having regard to both Directive 95/46 and Regulation 2016/679.

Question 1(a) and (c)

44. By Question 1(a) and (c), the referring court asks, in essence, whether Article 2(f) and Article 5(3) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46 and Article 6(1)(a) of Regulation 2016/679, must be interpreted as meaning that the consent referred to in those provisions is validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent.

45. As a preliminary matter, it is important to note that, according to the order for reference, the cookies likely to be placed on the terminal equipment of a user participating in the promotional lottery organised by Planet49 contain a number which is assigned to the registration data of that user, who must enter his or her name and address in the registration form for the lottery. The referring court adds that, by linking that number with that data, a connection between a person to the data stored by the cookies arises if the user uses the internet, such that the collection of that data by means of cookies is a form of processing of personal data. Those statements were confirmed by Planet49, which noted in its written observations that the consent to which the second checkbox refers is intended to authorise the collection and processing of personal data, not anonymous data.

46. On the basis of those explanations, it should be noted that, in accordance with Article 5(3) of Directive 2002/58, Member States are to ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a user is only allowed on condition that the user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46, inter alia, about the purposes of the processing.

49. As regards the wording of Article 5(3) of Directive 2002/58, it should be made clear that, although that provision states expressly that the user must have 'given his or her consent' to the storage of and access to cookies on his or her terminal equipment, that provision does not, by contrast, indicate the way in which that consent must be given. The wording 'given his or her consent' does, however, lend itself to a literal interpretation according to which action is required on the part of the user in order to give his or her consent. In that regard, it is clear from recital 17 of Directive 2002/58 that, for the purposes of that directive, a user's consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including 'by ticking a box when visiting an internet website.'

51. Article 2(h) of Directive 95/46 defines 'the data subject's consent' as being 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'

52. Thus, as the Advocate General stated in point 60 of his Opinion, the requirement of an 'indication' of the data subject's wishes clearly points to active, rather than passive, behaviour. However, consent given in the form of a preselected tick in a checkbox does not imply active behaviour on the part of a website user.

53. That interpretation is borne out by Article 7 of Directive 95/46, which sets out an exhaustive list of cases in which the processing of personal data can be regarded as lawful.

54. In particular, Article 7(a) of Directive 95/46 provides that the data subject's consent may make such processing lawful provided that the data subject has given his or her consent 'unambiguously.' Only active behaviour on the part of the data subject with a view to giving his or her consent may fulfil that requirement.

55. In that regard, it would appear impossible in practice to ascertain objectively whether a website user had actually given his or her consent to the processing of his or her personal data by not deselecting a pre-ticked checkbox nor, in any event, whether that consent had been informed. It is not inconceivable that a user would not have read the information accompanying the preselected checkbox, or even would not have noticed that checkbox, before continuing with his or her activity on the website visited.

57. As regards the foregoing, the consent referred to in Article 2(f) and Article 5(3) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46, is therefore not validly constituted if the storage of information, or access to information already stored in an website user's terminal equipment, is permitted by way of a checkbox pre-ticked by the service provider which the user must deselect to refuse his or her consent.

58. It should be added that the indication of the data subject's wishes referred to in Article 2(h) of Directive 95/46 must, inter alia, be 'specific' in the sense that it must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes.

59. In the present case, contrary to what Planet49 claims, the fact that a user selects the button to participate in the promotional lottery organised by that company cannot therefore be sufficient for it to be concluded that the user validly gave his or her consent to the storage of cookies.

60. A fortiori, the preceding interpretation applies in the light of Regulation 2016/679.

61. As the Advocate General stated, in essence, in point 70 of his Opinion, the wording of Article 4(11) of Regulation 2016/679, which defines the 'data subject's consent' for the purposes of that regulation and, in particular, of Article 6(1)(a) thereof, to which Question 1(c) refers, appears even more stringent than that of Article 2(h) of Directive 95/46 in that it requires a 'freely given, specific, informed and unambiguous' indication of the data subject's wishes in the form of a statement or of 'clear affirmative action' signifying agreement to the processing of the personal data relating to him or her.

62. Active consent is thus now expressly laid down in Regulation 2016/679. It should be noted in that regard that, according to recital 32 thereof, giving consent could include ticking a box when visiting an internet website. On the other hand, that recital expressly precludes 'silence, pre-ticked boxes or inactivity' from constituting consent.

63. It follows that the consent . . . is not validly constituted if the storage of information, or access to information already stored in the website user's terminal equipment, is permitted by way of a pre-ticked checkbox which the user must deselect to refuse his or her consent.

Question 1(b)

66. By Question 1(b), the referring court wishes to know, in essence, whether Article 2(f) and Article 5(3) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46 and Article 6(1)(a) of Regulation 2016/679, must be interpreted differently according to whether or not the information stored or accessed on a website user's terminal equipment is personal data within the meaning of Directive 95/46 and Regulation 2016/679.

67. As stated in paragraph 45 above, the storage of cookies at issue in the main proceedings amounts to a processing of personal data.

68. That being the case, the Court notes, in any event, that Article 5(3) of Directive 2002/58 refers to 'the storing of information' and 'the gaining of access to information already stored,' without characterising that information or specifying that it must be personal data.

69. As the Advocate General stated in point 107 of his Opinion, that provision aims to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data.

70. That interpretation is borne out by recital 24 of Directive 2002/58, according to which any information stored in the terminal equipment of users of electronic communications networks are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. That protection applies to any information stored in such terminal equipment, regardless of whether or not it is personal data, and is intended, in particular, as is clear from that recital, to protect users from the risk that hidden identifiers and other similar devices enter those users' terminal equipment without their knowledge.

71. In the light of the foregoing considerations, the answer to Question 1(b) is that Article 2(f) and Article 5(3) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46 and Article 4(11) and Article 6(1)(a) of Regulation 2016/679, are not to be interpreted differently according to whether or not the information stored or accessed on a website user's terminal equipment is personal data within the meaning of Directive 95/46 and Regulation 2016/679.

Question 2

72. By Question 2, the referring court asks, in essence, whether Article 5(3) of Directive 2002/58 must be interpreted as meaning that the information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.

73. As has already been made clear in paragraph 46 above, Article 5(3) of Directive 2002/58 requires that the user concerned has given his or her consent, having been provided with clear and comprehensive information, 'in accordance with Directive [95/46],' inter alia, about the purposes of the processing.

74. As the Advocate General stated in point 115 of his Opinion, clear and comprehensive information implies that a user is in a position to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed. It must be clearly comprehensible and sufficiently detailed so as to enable the user to comprehend the functioning of the cookies employed.

75. In a situation such as that at issue in the main proceedings, in which, according to the file before the Court, cookies aim to collect information for advertising purposes relating to the products of partners of the organiser of the promotional lottery, the duration of the operation of the cookies and whether or not third parties may have access to those cookies form part of the clear and comprehensive information which must be provided to the user in accordance with Article 5(3) of Directive 2002/58.

76. In that regard, it should be made clear that Article 10 of Directive 95/46, to which Article 5(3) of Directive 2002/58 and Article 13 of Regulation 2016/679 refer, lists the information with which the controller must provide a data subject from whom data relating to himself are collected.

77. That information includes, inter alia, under Article 10 of Directive 95/46, in addition to the identity of the controller and the purposes of the processing for which the data are intended, any further information such as the recipients or categories of recipients of the data in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

78. Although the duration of the processing of the data is not included as part of that information, it is, however, clear from the words 'at least' in Article 10 of Directive 95/46 that that information is not listed exhaustively. Information on the duration of the operation of cookies must be regarded as meeting the requirement of fair data processing provided for in that article in that, in a situation such as that at issue in the main proceedings, a long, or even unlimited, duration means collecting a large amount of information on users' surfing behaviour and how often they may visit the websites of the organiser of the promotional lottery's advertising partners.

79. That interpretation is borne out by Article 13(2)(a) of Regulation 2016/679, which provides that the controller must, in order to ensure fair and transparent processing, provide the data subject with information relating, inter alia, to the period for which the personal data will be stored, or if that is not possible, to the criteria used to determine that period.

80. As to whether or not third parties may have access to cookies, that is information included within the information referred to in Article 10(c) of Directive 95/46 and in Article 13(1)(e) of Regulation 2016/679, since those provisions expressly refer to the recipients or categories of recipients of the data.

81. In the light of the foregoing considerations, the answer to Question 2 is that Article 5(3) of Directive 2002/58 must be interpreted as meaning that the information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.

On those grounds, the Court (Grand Chamber) hereby rules:

1. [T]hat the consent referred to in those provisions is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent.

2. [That the restrictions on cookies] are not to be interpreted differently according to whether or not the information stored or accessed on a website user's terminal equipment is personal data within the meaning of Directive 95/46 and Regulation 2016/679.

3. Article 5(3) of Directive 2002/58, as amended by Directive 2009/136, must be interpreted as meaning that the information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.

Notes

1. Most basically, *Planet49* applies the rigorous definition of consent from GDPR. GDPR states that consent must be "freely given, specific, informed and unambiguous" and the result of "clear affirmative action." Not deselecting a prechecked box does not qualify. Also, for consent to be "informed" the court holds that it must include both information about the duration of cookies as well as whether third parties will have access to them.

Given the difficulty of obtaining and relying on consent as a lawful basis for processing data, there has been considerable interest in alternative bases. In the below *Meta* case, the European Court of Justice examined whether a contractual necessity basis or a legitimate interest of the controller basis would allow for broad processing of personal data.

Meta v Bundeskartellamt, No. C-252/21, E.C.J. (2023)

1. This request for a preliminary ruling concerns the interpretation of [GDPR]

2. The request has been made in proceedings between Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd, and Facebook Deutschland GmbH, on the one hand, and the Bundeskartellamt (Federal Cartel Office, Germany), on the other, concerning the decision by which the latter prohibited those companies from processing certain personal data as provided for in the general terms of use of the social network Facebook ('the general terms').

The dispute in the main proceedings and the questions referred for a preliminary ruling

26. Meta Platforms Ireland operates the online social network Facebook within the European Union and promotes, inter alia via www.facebook.com, services that are free of charge for private users. Other undertakings of the Meta group offer, within the European Union, other online services, including Instagram, WhatsApp, Oculus and – until 13 March 2020 – Masquerade.

27. The business model of the online social network Facebook is based on financing through online advertising, which is tailored to the individual users of the social network according, inter alia, to their consumer behaviour, interests, purchasing power and personal situation. Such advertising is made possible in technical terms by the automated production of detailed profiles in respect of the network users and the users of the online services offered at the level of the Meta group. To that end, in addition to the data provided by the users directly when they sign up for the online services concerned, other user- and device-related data are also collected on and off that social network and the online services provided by the Meta group, and linked to their various user accounts. The aggregate view of the data allows detailed conclusions to be drawn about those users' preferences and interests.

28. For the processing of those data, Meta Platforms Ireland relies on the user agreement to which the users of the social network Facebook adhere when they click on the 'Sign up' button, thereby accepting the general terms drawn up by that company. Acceptance of those terms is necessary in order to be able to use the social network Facebook. With regard to the processing of personal data, the general terms refer to that company's data and cookies policies. According to those policies, Meta Platforms Ireland collects user- and device-related data about user activities on and off the social network and links the data with the Facebook accounts of the users concerned. The latter data, relating to activities outside the social network ('the off-Facebook data'), are data concerning visits to third-party webpages and apps, which are linked to Facebook through programming interfaces – 'Facebook Business Tools' – as well as data concerning the use of other online services belonging to the Meta group, including Instagram, WhatsApp, Oculus and – until 13 March 2020 – Masquerade.

29. The Federal Cartel Office brought proceedings against Meta Platforms, Meta Platforms Ireland and Facebook Deutschland, as a result of which it essentially prohibited those companies from making, in the general terms, the use of the social network Facebook by private users resident in Germany subject to the processing of their off-Facebook data and from processing the data without their consent on the basis of the general terms in force at the time. In addition, it required them to adapt those general terms in such a way that it is made clear that those data will neither be collected, nor linked with Facebook user accounts nor used without the consent of the user concerned, and it clarified the fact that such a consent is not valid if it is a condition for using the social network.

30. The Federal Cartel Office based its decision on the fact that the processing of the data of the users concerned, as provided for in the general terms and implemented by Meta

Platforms Ireland, constituted an abuse of that company's dominant position on the market for online social networks for private users in Germany. In particular, according to the Federal Cartel Office, those general terms, as a result of that dominant position, constitute an abuse since the processing of the off-Facebook data that they provide for is not consistent with the underlying values of the GDPR and, in particular, it cannot be justified in the light of Article 6(1) and Article 9(2) of that regulation.

31. On 11 February 2019, Meta Platforms, Meta Platforms Ireland and Facebook Deutschland brought an action against the decision of the Federal Cartel Office before the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany).

32. On 31 July 2019, Meta Platforms Ireland introduced new general terms expressly stating that the user, instead of paying to use Facebook products, agrees to being shown advertisements.

33. Furthermore, since 28 January 2020, Meta Platforms has been offering, at a global level, '*Off-Facebook Activity*', which allows the users of the social network Facebook to view a summary of the information about them that Meta group companies obtain in relation to their activities on other websites and apps, and to disconnect the data about past and future activities from their Facebook.com account if they so wish.

The questions referred

Question 2 [Does using the web tracking data count as processing special category data? If so, if the data effectively public?]

64. By Question 2(a), the referring court asks, in essence, whether Article 9(1) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories referred to in that provision relate and, as the case may be, enters information into them when registering or when placing online orders, the processing of personal data by the operator of that online social network, which entails the collection – by means of integrated interfaces, cookies or similar storage technologies – of data from visits to those sites and apps and of the information entered by the user, the linking of all those data with the user's social network account and the use of those data by that operator, must be regarded as 'processing of special categories of personal data' within the meaning of that provision, which is in principle prohibited, subject to the derogations provided for in Article 9(2).

65. If so, the referring court asks, in essence, by Question 2(b), whether Article 9(2)(e) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which the categories set out in Article 9(1) of the GDPR relate, enters information into those sites or apps or clicks or taps on the buttons integrated into them, such as the 'Like' or 'Share' buttons or the buttons enabling the user to identify himself or herself on those sites or apps using the login credentials linked to his or her online social network user account, his or her telephone number or email address, the user is deemed to have manifestly made public, within the meaning of the first of those provisions, the data collected on that occasion by the operator of that online social network via cookies or similar storage technologies.

Question 2(a)

66. Recital 51 of the GDPR states that personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. That recital further states that such personal data should not be processed unless processing is allowed in the specific cases set out in that regulation.

67. In that context, Article 9(1) of the GDPR lays down the principle that the processing of special categories of personal data listed therein is prohibited. This includes data revealing

racial or ethnic origin, political opinions, religious beliefs and data concerning health or a natural person's sex life or sexual orientation.

72. . . . it will be for the referring court to determine whether the data thus collected, on their own or by linking them with the Facebook accounts of the users concerned, actually allow such information to be revealed, irrespective of whether that information concerns a user of that network or any other natural person. However, given the referring court's questions, it should be made clear that it appears, subject to verification by that court, that the processing of data relating to visits to the websites or apps in question may, in certain cases, reveal such information without it being necessary for those users to enter information into them when they register or place online orders.

73. In the light of the foregoing, the answer to Question 2(a) is that Article 9(1) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories referred to in that provision relate and, as the case may be, enters information into them when registering or when placing online orders, the processing of personal data by the operator of that online social network, which entails the collection – by means of integrated interfaces, cookies or similar storage technologies – of data from visits to those sites and apps and of the information entered by the user, the linking of all those data with the user's social network account and the use of those data by that operator, must be regarded as 'processing of special categories of personal data' within the meaning of that provision, which is in principle prohibited, subject to the derogations provided for in Article 9(2), where that data processing allows information falling within one of those categories to be revealed, irrespective of whether that information concerns a user of that network or any other natural person.

Question 2(b)

74. As regards Question 2(b), as reformulated in paragraph 65 above and which relates to the derogation laid down in Article 9(2)(e) of the GDPR, it must be recalled that, under that provision, the fundamental prohibition of any processing of special categories of personal data, established in Article 9(1) of the GDPR, does not apply in the circumstance where the processing relates to personal data which are 'manifestly made public by the data subject'.

75. As a preliminary point, it should be noted that, first, the derogation applies only to data which are manifestly made public 'by the data subject'. Accordingly, it is not applicable to data concerning persons other than the person who made those data public.

76. Second, in so far as it provides for an exception to the principle that the processing of special categories of personal data is prohibited, Article 9(2) of the GDPR must be interpreted strictly.

77. It follows that, for the purposes of the application of the exception laid down in Article 9(2)(e) of the GDPR, it is important to ascertain whether the data subject had intended, explicitly and by a clear affirmative action, to make the personal data in question accessible to the general public.

78. In that regard, as regards, first, visits to websites or apps to which one or more of the categories referred to in Article 9(1) of the GDPR relate, it should be noted that the user concerned does not in any way thereby intend to make public the fact that he or she has visited those sites or apps and the data from those visits which can be linked to his or her person. The latter can at most expect the operator of the site or app to have access to those data and to share them, as the case may be and subject to that user's explicit consent, with certain third parties and not with the general public.

79. Thus, it cannot be inferred from the mere visit to such websites or apps by a user that the personal data in question were manifestly made public by that user within the meaning of Article 9(2)(e) of the GDPR.

80. Second, as regards the entering of information into those websites or apps and the clicking or tapping on buttons integrated into them, such as the 'Like' or 'Share' buttons or buttons enabling the user to identify himself or herself on a website or app using the login credentials linked to his or her Facebook user account, his or her telephone number or email address, it should be noted that these actions mean that the user interacts with the website or app in question, and, as the case may be, the website of the online social network, whereby the extent to which that interaction is public may vary in that it may be determined by the individual settings chosen by that user.

81. In those circumstances, it is for the referring court to ascertain whether it is possible for the users concerned to decide, on the basis of settings selected with full knowledge of the facts, whether to make the information entered into the websites or apps in question and the data from clicking or tapping on buttons integrated into them accessible to the general public or, rather, to a more or less limited number of selected persons.

[Questions 3 and 4. Can the processing of such personal data be justified as necessary for the performance of a contract or the legitimate interests of the controller?]

86. By Questions 3 and 4, which it is appropriate to examine together, the referring court asks, in essence, whether and under what conditions points (b) and (f) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of such data, may be considered to be necessary for the performance of a contract to which the data subjects are party, within the meaning of point (b), or for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of point (f). That court asks, in particular, whether, to that end, certain interests which it explicitly lists constitute 'legitimate interests' within the meaning of the latter provision.

97. As regards, in the first place, point (b) of the first subparagraph of Article 6(1) of the GDPR, that provision provides that processing of personal data is lawful if it is 'necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract'.

98. In that regard, in order for the processing of personal data to be regarded as necessary for the performance of a contract, within the meaning of that provision, it must be objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject. The controller must therefore be able to demonstrate how the main subject matter of the contract cannot be achieved if the processing in question does not occur.

99. The fact that such processing may be referred to in the contract or may be merely useful for the performance of the contract is, in itself, irrelevant in that regard. The decisive factor for the purposes of applying the justification set out in point (b) of the first subparagraph of Article 6(1) of the GDPR is rather that the processing of personal data by the controller must be essential for the proper performance of the contract concluded between the controller and the data subject and, therefore, that there are no workable, less intrusive alternatives.

100. In that regard, as the Advocate General observed, where the contract consists of several separate services or elements of a service that can be performed independently of one

another, the applicability of point (b) of the first subparagraph of Article 6(1) of the GDPR should be assessed in the context of each of those services separately.

101. In the present case, in the context of the justifications that are capable of falling within the scope of that provision, the referring court mentions, as elements intended to ensure the proper performance of the contract concluded between Meta Platforms Ireland and its users, personalised content and the consistent and seamless use of the Meta group's own services.

102. As regards, first, the justification based on personalised content, it is important to note that, although such a personalisation is useful to the user, in so far as it enables the user, inter alia, to view content corresponding to a large extent to his or her interests, the fact remains that, subject to verification by the referring court, personalised content does not appear to be necessary in order to offer that user the services of the online social network. Those services may, where appropriate, be provided to the user in the form of an equivalent alternative which does not involve such a personalisation, such that the latter is not objectively indispensable for a purpose that is integral to those services.

103. As regards, second, the justification based on the consistent and seamless use of the Meta group's own services, it is apparent from the file before the Court that there is no obligation to subscribe to the various services offered by the Meta group in order to create a user account in the social network Facebook. The various products and services offered by that group can be used independently of each other and the use of each product or service is based on the conclusion of a separate user agreement.

104. Therefore, and subject to verification by the referring court, the processing of personal data from services offered by the Meta group, other than the online social network service, does not appear to be necessary for the latter service to be provided.

105. As regards, in the second place, point (f) of the first subparagraph of Article 6(1) of the GDPR, that provision provides that the processing of personal data is lawful only if it is 'necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child'.

106. As the Court has already held, that provision lays down three cumulative conditions so that the processing of personal data covered by that provision is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or fundamental freedoms and rights of the person concerned by the data protection do not take precedence over the legitimate interest of the controller or of a third party.

107. First, with regard to the condition relating to the pursuit of a legitimate interest, it must be stated that, according to Article 13(1)(d) of the GDPR, it is the responsibility of the controller, at the time when personal data relating to a data subject are collected from that person, to inform him or her of the legitimate interests pursued where that processing is based on point (f) of the first subparagraph of Article 6(1) of that regulation.

108. Second, with regard to the condition that the processing of personal data be necessary for the purposes of the legitimate interests pursued, that condition requires the referring court to ascertain that the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter.

109. In this context, it should also be recalled that the condition relating to the need for processing must be examined in conjunction with the 'data minimisation' principle enshrined

in Article 5(1)(c) of the GDPR, in accordance with which personal data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.

110. Third, with regard to the condition that the interests or fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interests of the controller or of a third party, the Court has already held that that condition entails a balancing of the opposing rights and interests at issue which depends in principle on the specific circumstances of the particular case and that, consequently, it is for the referring court to carry out that balancing exercise, taking account of those specific circumstances.

111. In this respect, it is apparent from the very wording of point (f) of the first subparagraph of Article 6(1) of the GDPR that it is necessary, in such a balancing exercise, to pay particular attention to the situation where the data subject is a child. According to recital 38 of that regulation, children merit specific protection with regard to the processing of their personal data because they may be less aware of the risks, consequences and safeguards concerned and of their rights related to such processing of personal data. Thus, such specific protection should, in particular, apply to the processing of personal data of children for the purposes of marketing or creating personality or user profiles or offering services aimed directly at children.

112. Furthermore, as can be seen from recital 47 of the GDPR, the interests and fundamental rights of the data subject may in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect such processing.

113. In the present case, in the context of the justifications that are capable of falling within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR, the referring court mentions personalised advertising, network security, product improvement, the sharing of informing with law-enforcement agencies, the fact that the user is a minor, research and innovation for social good and the offer of services for commercial communication intended for the user and of analytics tools intended for advertisers and other business partners, enabling them to evaluate their performance.

115. First, with regard to personalised advertising, it must be borne in mind that, according to recital 47 of the GDPR, the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest of the controller.

116. However, such processing must also be necessary in order to achieve that interest and the interests or fundamental freedoms and rights of the data subject must not override that interest. In the context of that balancing of the opposing rights at issue, namely, those of the controller, on the one hand, and those of the data subject, on the other, account must be taken, as has been noted in paragraph 112 above, in particular of the reasonable expectations of the data subject as well as the scale of the processing at issue and its impact on that person.

117. In this regard, it is important to note that, despite the fact that the services of an online social network such as Facebook are free of charge, the user of that network cannot reasonably expect that the operator of the social network will process that user's personal data, without his or her consent, for the purposes of personalised advertising. In those circumstances, it must be held that the interests and fundamental rights of such a user override the interest of that operator in such personalised advertising by which it finances its activity, with the result that the processing by that operator for such purposes cannot fall within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR.

118. Furthermore, the processing at issue in the main proceedings is particularly extensive since it relates to potentially unlimited data and has a significant impact on the user,

a large part – if not almost all – of whose online activities are monitored by Meta Platforms Ireland, which may give rise to the feeling that his or her private life is being continuously monitored.

119. Second, as regards the objective of ensuring network security, that objective, as stated in recital 49 of the GDPR, constitutes a legitimate interest of Meta Platforms Ireland, capable of justifying the processing operation at issue in the main proceedings.

120. However, as regards the need for that processing for the purposes of that legitimate interest, the referring court will have to ascertain whether and to what extent the processing of personal data collected from sources outside the social network Facebook is actually necessary to ensure that the internal security of that network is not compromised.

121. In that context, as noted in paragraphs 108 and 109 above, it will also have to ascertain whether the legitimate data processing interest pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental freedoms and rights of the data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter and whether the 'data minimisation' principle enshrined in Article 5(1)(c) of the GDPR has been observed.

122. Third, as regards the 'product improvement' objective, it cannot be ruled out from the outset that the controller's interest in improving the product or service with a view to making it more efficient and thus more attractive can constitute a legitimate interest capable of justifying the processing of personal data and that such processing may be necessary in order to pursue that interest.

123 However, subject to final assessment by the referring court in that respect, it appears doubtful whether, as regards the data processing at issue in the main proceedings, the 'product improvement' objective, given the scale of that processing and its significant impact on the user, as well as the fact that the user cannot reasonably expect those data to be processed by Meta Platforms Ireland, may override the interests and fundamental rights of such a user, particularly in the case where that user is a child.

124. Fourth, as regards the objective referred to by the referring court, relating to the sharing of information with law-enforcement agencies in order to prevent, detect and prosecute criminal offences, it must be held that that objective is not capable, in principle, of constituting a legitimate interest pursued by the controller. A private operator such as Meta Platforms Ireland cannot rely on such a legitimate interest, which is unrelated to its economic and commercial activity.

125. In the light of all the foregoing, the answer to Questions 3 and 4 is that point (b) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, can be regarded as necessary for the performance of a contract to which the data subjects are party, within the meaning of that provision, only on condition that the processing is objectively indispensable for a purpose that is integral to the contractual obligation intended for those users, such that the main subject matter of the contract cannot be achieved if that processing does not occur.

126. Point (f) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that such processing can be regarded as necessary for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of that provision, only on condition that the operator has informed the users from whom the data have been

collected of a legitimate interest that is pursued by the data processing, that such processing is carried out only in so far as is strictly necessary for the purposes of that legitimate interest and that it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of those users do not override that legitimate interest of the controller or of a third party.

Question 6 [Is Meta's dominant position in the social media space relevant to the consideration of whether consent was freely given?]

140. By Question 6, the referring court asks, in essence, whether point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR must be interpreted as meaning that consent given by the user of an online social network to the operator of such a network may be regarded as satisfying the conditions of validity laid down in Article 4(11) of that regulation, in particular the condition that that consent must be freely given, where that operator holds a dominant position on the market for online social networks.

147. In that regard, it should be noted that, admittedly, the fact that the operator of an online social network, as controller, holds a dominant position on the social network market does not, as such, prevent the users of that social network from validly giving their consent, within the meaning of Article 4(11) of the GDPR, to the processing of their personal data by that operator.

148. The fact remains that, as the Advocate General observed, in essence, such a circumstance must be taken into consideration in assessing whether the user of that network has validly and, in particular, freely given consent, since that circumstance is liable to affect the freedom of choice of that user, who might be unable to refuse or withdraw consent without detriment, as stated in recital 42 of the GDPR.

149. Furthermore, the existence of such a dominant position may create a clear imbalance, within the meaning of recital 43 of the GDPR, between the data subject and the controller, that imbalance favouring, inter alia, the imposition of conditions that are not strictly necessary for the performance of the contract, which must be taken into account under Article 7(4) of that regulation. In that context, it must be borne in mind that, as stated in paragraphs 102 to 104 above, it does not appear, subject to verification by the referring court, that the processing at issue in the main proceedings is strictly necessary for the performance of the contract between Meta Platforms Ireland and the users of the social network Facebook.

150. Thus, those users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations.

151. Moreover, given the scale of the processing of the data in question and the significant impact of that processing on the users of that network as well as the fact that those users cannot reasonably expect data other than those relating to their conduct within the social network to be processed by the operator of that network, it is appropriate, within the meaning of recital 43, to have the possibility of giving separate consent for the processing of the latter data, on the one hand, and the off-Facebook data, on the other. It is for the referring court to ascertain whether such a possibility exists, in the absence of which the consent of those users to the processing of the off-Facebook data must be presumed not to be freely given.

152. Finally, it must be borne in mind that, pursuant to Article 7(1) of the GDPR, where processing is based on consent, it is the controller who bears the burden of demonstrating that the data subject has consented to the processing of his or her personal data.

153. It is in the light of those criteria and of a detailed examination of all the circumstances of the case that the referring court will have to determine whether the users of the social network Facebook have validly and, in particular, freely given their consent to the processing at issue in the main proceedings.

154. In the light of the foregoing, the answer to Question 6 is that point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR must be interpreted as meaning that the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent, within the meaning of Article 4(11) of that regulation, to the processing of their personal data by that operator. This is nevertheless an important factor in determining whether the consent was in fact validly and, in particular, freely given, which it is for that operator to prove.

Notes

1. GDPR's most basic provision is that one cannot process personal data *unless* there is some legal basis for doing so. The list of permissible justifications of processing is not overly short, but decision after decision has construed the justifications narrowly. Here, the critical paragraphs are 97 through 104. From Meta's perspective, broad processing of personal data is key to its business model. Consider why the Court of Justice thinks that it is not necessary to the contract. It is looking for signs that the processing is "objectively indispensable." That the contract's purpose cannot be achieved but-for the processing. That the inability to process may cut substantially into Meta's profits does not meet those thresholds.
2. Further, Meta's efforts to justify the processing based on its own legitimate interests fall victim to difficult balancing tests. Meta does have several legitimate interests here: promoting data security, better targeting advertising, and product improvement. But the court held that consumers reasonable expectations did not include highly personalized advertising without prior consent, especially given the breadth of data available to Facebook. The other rationales also needed to be balanced against consumer privacy expectations, and the court appears skeptical that they can justify broad processing.
3. These twin holdings limiting both the contract necessity and legitimate business interest justifications for data processing may substantially affect the ability of platforms to lawfully process data for use in personalized advertising. They may, in fact, be driven back to relying on informed consent, which is much more challenging under GDPR.[259]

D. GDPR and International Data Transfers

GDPR imposes strict rules on the transfer of personal data outside the EU to ensure that data protection is not undermined when data is exported to jurisdictions with lower privacy standards. Transfers are permitted under the following conditions:

- When there has been an adequacy decision by European Commission approving the data protection standards of the receiving jurisdiction.
- When, in the absence of an adequacy decision, appropriate safeguards are in place, such as binding corporate rules or "standard contractual clauses." Standard contractual

[259] For further discussion of this case and its implications for platforms, see Nikolas Guggenberger, *Consent as Friction,* 66 B.C. L. REV. (forthcoming 2025),

clauses of model contract provisions that have been pre-approved by the European Commission as compliant with GDPR.[260]

As of 2024, the European Commission has recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States (commercial organizations participating in the EU-US Data Privacy Framework), and Uruguay as providing adequate protection.[261]

Maximilian Schrems, an Austrian privacy activist, has repeatedly challenged the transfer of EU personal information to the United States, however. His original complaint, filed in 2013, alleged concern that his data could be accessed by the FBI and NSA when it was transferred to the United States and that, under the then-existing Safe Harbor Decision of 2000, he did not have an effective means of challenging this potential access. Specifically, oversight of the intelligence services' actions is carried out within the framework of an *ex parte* and secret procedure (see Chapter 4 for details), denying EU citizens the ability to defend their privacy in court. In 2015, the Court of Justice of the European Union held, first, that it could review the European Commission's decision to approve the Safe Harbor framework and, second, that the framework did not provide an adequate level of privacy protection, so transfers could not be completed under its authority (Schrems I).[262]

Following the rejection of the Safe Harbor Privacy Principles, a new legal framework called the EU–US Privacy Shield was created and went into effect in 2016. Schrems again sued challenging this framework, and it was declared invalid on July 16, 2020 (Schrems II). The replacement for the Privacy Shield, the Trans-Atlantic Data Privacy Framework, was approved by the Commission in 2022. Schrems's challenge to this new framework is now pending (Schrems III).

Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximilian Schrems (*Schrems II*), No. C-311/18, E.C.J. (2020)

42. In the judgment of 6 October 2015, *Schrems I,* the Court declared Commission Decision . . . on the adequacy of the protection provided by the safe harbour privacy principles . . . , in which the Commission had found that that third country ensured an adequate level of protection, invalid.

43. Following the delivery of that judgment, the Commission adopted the Privacy Shield Decision . . . .

> 'The Commission has assessed the limitations and safeguards available in U.S. law as regards access and use of personal data transferred under the EU–U.S. Privacy Shield by U.S. public authorities for national security, law enforcement and other public interest purposes. In addition, the U.S. government, through its Office of the Director of National Intelligence (ODNI) . . . . , has provided the Commission with detailed representations and commitments that are contained in Annex VI to this decision. By letter signed by the Secretary of State and attached as Annex III to this decision the U.S. government has also committed to create a new oversight mechanism for national security interference, the Privacy Shield Ombudsperson, who is independent from the Intelligence Community.

---

[260] For more information, see 2021 O.J. (L 199) 31 at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

[261] *Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection*, EUR. UNION, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[262] *Maximilian Schrems v. Data Protection Commissioner*, No. C-362/14, E.C.J. (2015).

> Finally, a representation from the U.S. Department of Justice, contained in Annex VII to this decision, describes the limitations and safeguards applicable to access and use of data by public authorities for law enforcement and other public interest purposes. In order to enhance transparency and to reflect the legal nature of these commitments, each of the documents listed and annexed to this decision will be published in the U.S. Federal Register.'

The dispute in the main proceedings and the questions referred for a preliminary ruling

50. Mr. Schrems, an Austrian national residing in Austria, has been a user of the Facebook social network ('Facebook') since 2008.

51. Any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his or her registration, a contract with Facebook Ireland, a subsidiary of Facebook Inc. which is itself established in the United States. Some or all of the personal data of Facebook Ireland's users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing.

55. In his reformulated complaint lodged on 1 December 2015, Mr. Schrems claimed, inter alia, that United States law requires Facebook Inc. to make the personal data transferred to it available to certain United States authorities, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). He submitted that, since that data was used in the context of various monitoring programmes in a manner incompatible with Articles 7, 8 and 47 of the Charter, the SCC Decision cannot justify the transfer of that data to the United States. In those circumstances, Mr. Schrems asked the Commissioner to prohibit or suspend the transfer of his personal data to Facebook Inc.

The first question [Does GDPR apply to transfer of personal data to other countries where the data might be processed for public security, defense, and state security?]

80. By its first question, the referring court wishes to know, in essence, whether Article 2(1) and Article 2(2)(a), (b) and (d) of the GDPR, read in conjunction with Article 4(2) TEU, must be interpreted as meaning that that regulation applies to the transfer of personal data by an economic operator established in a Member State to another economic operator established in a third country, in circumstances where, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of that third country for the purposes of public security, defence and State security.

85. In the present case, since the transfer of personal data at issue in the main proceedings is from Facebook Ireland to Facebook Inc., namely between two legal persons, that transfer does not fall within Article 2(2)(c) of the GDPR, which refers to the processing of data by a natural person in the course of a purely personal or household activity. Such a transfer also does not fall within the exceptions laid down in Article 2(2)(a), (b) and (d) of that regulation, since the activities mentioned therein by way of example are, in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active.

86. The possibility that the personal data transferred between two economic operators for commercial purposes might undergo, at the time of the transfer or thereafter, processing for the purposes of public security, defence and State security by the authorities of that third country cannot remove that transfer from the scope of the GDPR.

87. Indeed, by expressly requiring the Commission, when assessing the adequacy of the level of protection afforded by a third country, to take account, inter alia, of 'relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation

of such legislation', it is patent from the very wording of Article 45(2)(a) of that regulation that no processing by a third country of personal data for the purposes of public security, defence and State security excludes the transfer at issue from the application of the regulation.

The second, third and sixth questions [How should the adequacy of standard contractual clauses be evaluated, and does it require consideration of the recipient country's laws?]

90. By its second, third and sixth questions, the referring court seeks clarification from the Court, in essence, on the level of protection required by Article 46(1) and Article 46(2)(c) of the GDPR in respect of a transfer of personal data to a third country based on standard data protection clauses. In particular, the referring court asks the Court to specify which factors need to be taken into consideration for the purpose of determining whether that level of protection is ensured in the context of such a transfer.

91. As regards the level of protection required, it follows from a combined reading of those provisions that, in the absence of an adequacy decision under Article 45(3) of that regulation, a controller or processor may transfer personal data to a third country only if the controller or processor has provided 'appropriate safeguards,' and on condition that 'enforceable data subject rights and effective legal remedies for data subjects' are available, such safeguards being able to be provided, inter alia, by the standard data protection clauses adopted by the Commission.

94. [A]lthough not requiring a third country to ensure a level of protection identical to that guaranteed in the EU legal order, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter.

95. In that context, recital 107 of the GDPR states that, where 'a third country, a territory or a specified sector within a third country . . . no longer ensures an adequate level of data protection . . . the transfer of personal data to that third country . . . should be prohibited, unless the requirements [of that regulation] relating to transfers subject to appropriate safeguards . . . are fulfilled.' To that effect, recital 108 of the regulation states that, in the absence of an adequacy decision, the appropriate safeguards to be taken by the controller or processor in accordance with Article 46(1) of the regulation must 'compensate for the lack of data protection in a third country' in order to 'ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union.'

102. The referring court also seeks to ascertain what factors should be taken into consideration for the purposes of determining the adequacy of the level of protection where personal data is transferred to a third country pursuant to standard data protection clauses adopted under Article 46(2)(c) of the GDPR.

104. The assessment required for that purpose in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country. As regards the latter, the factors to be taken into consideration in the context of Article 46 of that regulation correspond to those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.

105. Therefore, the answer to the second, third and sixth questions is that Article 46(1) and Article 46(2)(c) of the GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must

ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.

The eighth question [Need a competent supervisory authority suspend or prohibit a transfer of personal data to a third country when those clauses cannot be complied with by the receiving entity?]

106. By its eighth question, the referring court wishes to know, in essence, whether Article 58(2)(f) and (j) of the GDPR must be interpreted as meaning that the competent supervisory authority is required to suspend or prohibit a transfer of personal data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of the GDPR and by the Charter, cannot be ensured, or as meaning that the exercise of those powers is limited to exceptional cases.

110. Article 78(1) and (2) of the GDPR recognises the right of each person to an effective judicial remedy, in particular, where the supervisory authority fails to deal with his or her complaint. Recital 141 of that regulation also refers to that 'right to an effective judicial remedy in accordance with Article 47 of the Charter' in circumstances where that supervisory authority 'does not act where such action is necessary to protect the rights of the data subject.'

111. In order to handle complaints lodged, Article 58(1) of the GDPR confers extensive investigative powers on each supervisory authority. If a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. To that effect, Article 58(2) of that regulation lists the various corrective powers which the supervisory authority may adopt.

113. In that regard, . . . the supervisory authority is required, under Article 58(2)(f) and (j) of that regulation, to suspend or prohibit a transfer of personal data to a third country if, in its view, in the light of all the circumstances of that transfer, the standard data protection clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

115. In any event, the implementing power which Article 46(2)(c) of the GDPR grants to the Commission for the purposes of adopting standard data protection clauses does not confer upon it competence to restrict the national supervisory authorities' powers on the basis of Article 58(2) of that regulation. Moreover, as stated in recital 5 of Implementing Decision 2016/2297, the SCC Decision 'does not prevent a [supervisory authority] from exercising its powers to oversee data flows, including the power to suspend or ban a transfer of personal data when it determines that the transfer is carried out in violation of EU or national data protection law.'

116. It should, however, be pointed out that the powers of the competent supervisory authority are subject to full compliance with the decision in which the Commission finds, where

relevant, under the first sentence of Article 45(1) of the GDPR, that a particular third country ensures an adequate level of protection. In such a case, it is clear from the second sentence of Article 45(1) of that regulation, read in conjunction with recital 103 thereof, that transfers of personal data to the third country in question may take place without requiring any specific authorisation.

117. Under the fourth paragraph of Article 288 TFEU, a Commission adequacy decision is, in its entirety, binding on all the Member States to which it is addressed and is therefore binding on all their organs in so far as it finds that the third country in question ensures an adequate level of protection and has the effect of authorising such transfers of personal data.

118. Thus, until such time as a Commission adequacy decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, cannot adopt measures contrary to that decision [but the decision itself can be challenged].

121. In the light of the foregoing considerations, the answer to the eighth question is that Article 58(2)(f) and (j) of the GDPR must be interpreted as meaning that, unless there is a valid Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of the GDPR and by the Charter, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

The 7th and 11th questions [Can the standard contractual clauses be assessed independent of national laws?]

124. Article 1 of the SCC Decision provides that the standard data protection clauses set out in its annex are considered to offer adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals in accordance with the requirements of Article 26(2) of Directive 95/46. The latter provision was, in essence, reproduced in Article 46(1) and Article 46(2)(c) of the GDPR.

125. However, although those clauses are binding on a controller established in the European Union and the recipient of the transfer of personal data established in a third country where they have concluded a contract incorporating those clauses, it is common ground that those clauses are not capable of binding the authorities of that third country, since they are not party to the contract.

126. Therefore, although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses, there are others in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.

127. Thus, the question arises whether a Commission decision concerning standard data protection clauses, adopted pursuant to Article 46(2)(c) of the GDPR, is invalid in the absence, in that decision, of guarantees which can be enforced against the public authorities of the third countries to which personal data is or could be transferred pursuant to those clauses.

128. Article 46(1) of the GDPR provides that, in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject

rights and effective legal remedies for data subjects are available. According to Article 46(2)(c) of the GDPR, those safeguards may be provided by standard data protection clauses drawn up by the Commission. However, those provisions do not state that all safeguards must necessarily be provided for in a Commission decision such as the SCC Decision.

129. It should be noted in that regard that such a standard clauses decision differs from an adequacy decision adopted pursuant to Article 45(3) of the GDPR, which seeks, following an examination of the legislation of the third country concerned taking into account, inter alia, the relevant legislation on national security and public authorities' access to personal data, to find with binding effect that a third country, a territory or one or more specified sectors within that third country ensures an adequate level of protection and that the access of that third country's public authorities to such data does not therefore impede transfers of such personal data to the third country. Such an adequacy decision can therefore be adopted by the Commission only if it has found that the third country's relevant legislation in that field does in fact provide all the necessary guarantees from which it can be concluded that that legislation ensures an adequate level of protection.

132. Since by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries, . . . but that Article 44, Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, require that the level of protection of natural persons guaranteed by that regulation is not undermined, it may prove necessary to supplement the guarantees contained in those standard data protection clauses. In that regard, recital 109 of the regulation states that 'the possibility for the controller . . . to use standard data-protection clauses adopted by the Commission . . . should [not] prevent [it] . . . from adding other clauses or additional safeguards' and states, in particular, that the controller 'should be encouraged to provide additional safeguards . . . that supplement standard [data] protection clauses.'

133. It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.

135. Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned. That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data.

142. It follows that a controller established in the European Union and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned. The recipient is, where appropriate, under an obligation, under Clause 5(b), to inform the controller of any inability to comply with those clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract.

The 4th, 5th, 9th and 10th questions [Is the Privacy Shield adequate?]

150. By its ninth question, the referring court wishes to know, in essence, whether and to what extent findings in the Privacy Shield Decision to the effect that the United States ensures an adequate level of protection are binding on the supervisory authority of a Member State. By its 4th, 5th and 10th questions, that court asks, in essence, whether, in view of its own findings on US law, the transfer to that third country of personal data pursuant to the standard data protection clauses in the annex to the SCC Decision breaches the rights enshrined in Articles 7, 8 and 47 of the Charter and asks the Court, in particular, whether the introduction of the ombudsperson referred to in Annex III to the Privacy Shield Decision is compatible with Article 47 of the Charter.

163. The Commission found, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU–US Privacy Shield . . . .

164. However, the Privacy Shield Decision also states, in paragraph I.5. of Annex II, under the heading 'EU–U.S. Privacy Shield Framework Principles,' that adherence to those principles may be limited, inter alia, 'to the extent necessary to meet national security, public interest, or law enforcement requirements.' Thus, that decision lays down, as did Decision 2000/520, that those requirements have primacy over those principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard the principles without limitation where they conflict with the requirements and therefore prove incompatible with them.

165. In the light of its general nature, the derogation set out in paragraph I.5 of Annex II to the Privacy Shield Decision thus enables interference, based on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. More particularly, as noted in the Privacy Shield Decision, such interference can arise from access to, and use of, personal data transferred from the European Union to the United States by US public authorities through the PRISM and UPSTREAM surveillance programmes under Section 702 of the FISA and E.O. 12333.

166. In that context, in recitals 67 to 135 of the Privacy Shield Decision, the Commission assessed the limitations and safeguards available in US law, inter alia under Section 702 of the FISA, E.O. 12333 and PPD-28, as regards access to, and use of, personal data transferred under the EU–US Privacy Shield by US public authorities for national security, law enforcement and other public interest purposes.

167. Following that assessment, the Commission found that 'the United States ensures an adequate level of protection for personal data transferred from the [European] Union to self-certified organisations in the United States,' and, in recital 140 of the decision, it considered that, 'on the basis of the available information about the U.S. legal order, . . . any interference by U.S. public authorities with the fundamental rights of the persons whose data are transferred from the [European] Union to the United States under the Privacy Shield for national security, law enforcement or other public interest purposes, and the ensuing restrictions imposed on self-certified organisations with respect to their adherence to the Principles, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that there exists effective legal protection against such interference.'

The finding of an adequate level of protection

168. In the light of the factors mentioned by the Commission in the Privacy Shield Decision and the referring court's findings in the main proceedings, the referring court harbours doubts as to whether US law in fact ensures the adequate level of protection required under Article 45 of the GDPR, read in the light of the fundamental rights guaranteed in Articles 7, 8

and 47 of the Charter. In particular, that court considers that the law of that third country does not provide for the necessary limitations and safeguards with regard to the interferences authorised by its national legislation and does not ensure effective judicial protection against such interferences. As far as concerns effective judicial protection, it adds that the introduction of a Privacy Shield Ombudsperson cannot, in its view, remedy those deficiencies since an ombudsperson cannot be regarded as a tribunal within the meaning of Article 47 of the Charter.

171. The Court has held that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference.

172. However, the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society.

173. In this connection, it should also be observed that, under Article 8(2) of the Charter, personal data must, inter alia, be processed 'for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.'

174. Furthermore, in accordance with the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

175. Following from the previous point, it should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned.

176. Lastly, in order to satisfy the requirement of proportionality according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing.

177. To that effect, Article 45(2)(a) of the GDPR states that, in its assessment of the adequacy of the level of protection in a third country, the Commission is, in particular, to take account of 'effective and enforceable data subject rights' for data subjects whose personal data are transferred.

178. In the present case, the Commission's finding in the Privacy Shield Decision that the United States ensures an adequate level of protection for personal data essentially equivalent to that guaranteed in the European Union by the GDPR, read in the light of Articles 7 and 8 of the Charter, has been called into question, inter alia, on the ground that the interference arising from the surveillance programmes based on Section 702 of the FISA and

on E.O. 12333 are not covered by requirements ensuring, subject to the principle of proportionality, a level of protection essentially equivalent to that guaranteed by the second sentence of Article 52(1) of the Charter. It is therefore necessary to examine whether the implementation of those surveillance programmes is subject to such requirements, and it is not necessary to ascertain beforehand whether that third country has complied with conditions essentially equivalent to those laid down in the first sentence of Article 52(1) of the Charter.

179. In that regard, as regards the surveillance programmes based on Section 702 of the FISA, the Commission found, in recital 109 of the Privacy Shield Decision, that, according to that article, 'the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications prepared by the Attorney General and the Director of National Intelligence (DNI).' As is clear from that recital, the supervisory role of the FISC is thus designed to verify whether those surveillance programmes relate to the objective of acquiring foreign intelligence information, but it does not cover the issue of whether 'individuals are properly targeted to acquire foreign intelligence information.'

180. It is thus apparent that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances and as the Advocate General stated, in essence, . . . that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter, . . . according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards.

181. According to the findings in the Privacy Shield Decision, the implementation of the surveillance programmes based on Section 702 of the FISA is, indeed, subject to the requirements of PPD-28. However, although the Commission stated, that such requirements are binding on the US intelligence authorities, the US Government has accepted, in reply to a question put by the Court, that PPD-28 does not grant data subjects actionable rights before the courts against the US authorities. Therefore, the Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter, contrary to the requirement in Article 45(2)(a) of the GDPR . . . .

182. As regards the monitoring programmes based on E.O. 12333, it is clear from the file before the Court that that order does not confer rights which are enforceable against the US authorities in the courts either.

183. It should be added that PPD-28, with which the application of the programmes referred to in the previous two paragraphs must comply, allows for '"bulk" collection . . . of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target . . . to focus the collection, as stated in a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision. That possibility, which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data.

184. It follows therefore that neither Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from

the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary.

185. In those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter.

192. Furthermore, as regards both the surveillance programmes based on Section 702 of the FISA and those based on E.O. 12333, it has been noted in paragraphs 181 and 182 above that neither PPD-28 nor E.O. 12333 grants data subjects rights actionable in the courts against the US authorities, from which it follows that data subjects have no right to an effective remedy.

193. The Commission found, however, in recitals 115 and 116 of the Privacy Shield Decision, that, as a result of the Ombudsperson Mechanism introduced by the US authorities, as described in a letter from the US Secretary of State to the European Commissioner for Justice, Consumers and Gender Equality from 7 July 2016, set out in Annex III to that decision, and of the nature of that Ombudsperson's role, in the present instance, a 'Senior Coordinator for International Information Technology Diplomacy,' the United States can be deemed to ensure a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter.

194. An examination of whether the ombudsperson mechanism which is the subject of the Privacy Shield Decision is in fact capable of addressing the Commission's finding of limitations on the right to judicial protection must, in accordance with the requirements arising from Article 47 of the Charter . . . , start from the premise that data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data.

195. In the letter referred to in paragraph 193 above, the Privacy Shield Ombudsperson, although described as 'independent from the Intelligence Community,' was presented as '[reporting] directly to the Secretary of State who will ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided.' Furthermore, in addition to the fact that, as found by the Commission in recital 116 of that decision, the Ombudsperson is appointed by the Secretary of State and is an integral part of the US State Department, there is, as the Advocate General stated . . . , nothing in that decision to indicate that the dismissal or revocation of the appointment of the Ombudsperson is accompanied by any particular guarantees, which is such as to undermine the Ombudsman's independence from the executive.

196. Similarly, as the Advocate General stated . . . , although recital 120 of the Privacy Shield Decision refers to a commitment from the US Government that the relevant component of the intelligence services is required to correct any violation of the applicable rules detected by the Privacy Shield Ombudsperson, there is nothing in that decision to indicate that that ombudsperson has the power to adopt decisions that are binding on those intelligence services and does not mention any legal safeguards that would accompany that political commitment on which data subjects could rely.

197. Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.

199. It follows that Article 1 of the Privacy Shield Decision is incompatible with Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter, and is therefore invalid.

200. Since Article 1 of the Privacy Shield Decision is inseparable from Articles 2 and 6 of, and the annexes to, that decision, its invalidity affects the validity of the decision in its entirety.

201. In the light of all of the foregoing considerations, it is to be concluded that the Privacy Shield Decision is invalid.

202. As to whether it is appropriate to maintain the effects of that decision for the purposes of avoiding the creation of a legal vacuum, the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR.

Notes

1. *Schrems II* is a complicated decision. Most basically, it invalidated the Privacy Shield, meaning that EU entities wishing to transfer data to the U.S. needed a different lawful basis for doing so. *Schrems II* did not invalidate the standard contractual clauses per se, but it did require controllers to make an assessment of whether a foreign company signing a contract containing such clauses would be able to actually abide by them. In short, is Facebook U.S. making promises it can keep when it tells Facebook Ireland/EU that it will not inappropriately share data with the U.S. government?
2. Following *Schrems II*, the Trans-Atlantic Data Privacy Framework (TADP) was created to replace the Privacy Shield. Implemented by Executive Order 14086 in 2022 and approved by the European Commission in 2023, TADP imposes two key reforms. First, TADP requires that "signals intelligence activities . . . be conducted only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorized" and only for a list of enumerated legitimate objectives. Second, the order created a new redress mechanism for EU residents that allows them to challenge use of their data in a newly created Data Protection Review Court. This court has extremely limited jurisdiction, however, and can only hear cases that have progressed through a convoluted process involving both EU data protection officials and the U.S. Office of the Director of National Intelligence. Whether this will count as an effective redress mechanism, as required by *Schrems II*, is unclear.
3. This interest in international data transfers is not limited to the EU. A number of countries, including the United States, are interested in the extent to which data on their citizens is also (or only) stored overseas. Sometimes the concern is that Country B will be able to access the data on Country A's citizens for national security purposes (think U.S. concerns about Chinese ownership of TikTok and telecom infrastructure). Sometimes the concern is that Country A will not be able to access the data on its own citizens if that data is solely available in Country B (think countries requiring that a copy of the data on their citizens be hosted locally). For more on these points, consider Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677 (2015).