

What is Privacy Law?

Matthew Kugler

Privacy Law & Regulation

HARVARD LAW REVIEW.

VOL. IV.

DECEMBER 15, 1890.

NO. 5.

THE RIGHT TO PRIVACY.

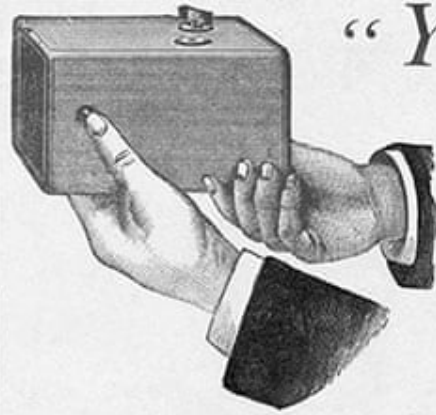
"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in *Millar v. Taylor*, 4 Burr. 2303, 2312.

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



The Kodak Camera



*“You press the button,
we do the rest.”*

OR YOU CAN DO IT YOURSELF.

The only camera that anybody
can use without instructions. As
convenient to carry as an ordinary
field glass World-wide success.

The Kodak is for sale by all Photo stock dealers.

Send for the Primer, free.

The Eastman Dry Plate & Film Co.

Price, \$25.00 — Loaded for 100 Pictures.

Re-loading, \$2.00.

ROCHESTER, N. Y.



Northwestern

Privacy's Advocates & Dissidents

Matthew Kugler

Privacy Law & Regulation

Privacy Benefits

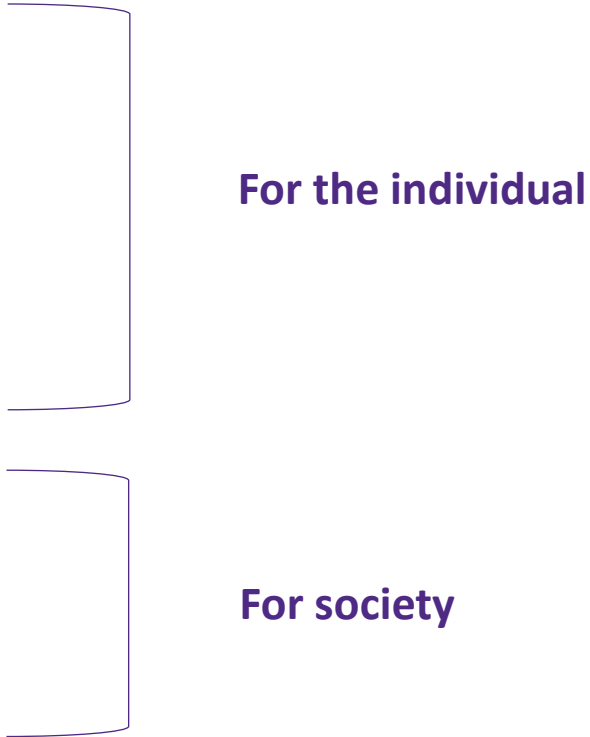
- Emotional release
- Selective disclosure; intimacy & emotional closeness
- Permissible deviations



For the individual

Privacy Benefits

- Emotional release
 - Selective disclosure; intimacy & emotional closeness
 - Permissible deviations
-
- Autonomy & societal change
 - Experimentation



The diagram consists of two large, light purple curly brackets on the right side of the slide. The top bracket groups the first three bullet points under the label 'For the individual'. The bottom bracket groups the last two bullet points under the label 'For society'.

For the individual

For society

Privacy Drawbacks



- Privacy allows for **social fraud**. Hiding who you are from people who have a right to know.
- Little sins matter. The supposedly harmless things you hide are not harmless.
- People can be trusted to decide what is relevant.

(Photo: Richard Posner)

JOB APPLICATION

☐ Have you ever been convicted
of a criminal offense?

Ban the BOX

THE BLOG

The Ugly Truth of Online Dating: Top 10 Lies Told by Internet Daters

Running an exclusive online dating site myself, I can attest to the constant work I'm doing to maintain the integrity of online dating communities by weeding out disingenuous profiles -- yes, surprise surprise! Online daters lie.

By Greg Hodge, Contributor
CEO, BeautifulPeople

10/10/2012 02:10pm ET | Updated December 10, 2012

This post was published on the now-closed HuffPost Contributor platform. Contributors control their own work and retain full copyright. Any copyright in this post should be considered as transferred to the author.

Everybody lies: What people are lying about on dating sites

October 10, 2017

Kaspersky Lab and B2B International jointly [researched](#) online dating site users' patterns of behavior and the threats they encounter. We found out what type of information users are prepared to share with strangers and why (and about what) so many of them lie.



Intrusion Upon Seclusion

Matthew Kugler

Privacy Law & Regulation

Intrusion Upon Seclusion

To prove intrusion upon seclusion, you must show:

- **intentional intrusion**
- upon the solitude or seclusion of another in his **private affairs** or concerns
- that is **highly offensive** to a reasonable person.

May be intrusions

- Entering a private place without permission
- Looking into a private place with binoculars
- Wiretapping
- Searching private documents

Likely not

- Photographing in public spaces
- Inspecting public records
- Knocking on their door or calling their phone during reasonable hours

Intrusion Upon Seclusion

To prove intrusion upon seclusion, you must show:

1. **intentional intrusion**
2. upon the **solitude or seclusion of another in his private affairs or concerns**
3. that is **highly offensive to a reasonable person**.

Safari Club v. Rudolph

- Was it an intrusion upon seclusion to record a conversation in a public restaurant?
- Turns on whether there was a reasonable expectation of privacy.
- Public setting, which counts against it being highly offensive.
- But not every conversation in public is not private.
- Messy issues of fact. Sent to the jury.

The Limited Private Sphere

Matthew Kugler

Privacy Law & Regulation

Public Disclosure of Private Facts

To prove public disclosure of private facts, you must show that someone:

1. Gave **publicity**
2. To a matter concerning the **private life** of another
3. that is **highly offensive to a reasonable person** and
4. is not of legitimate concern to the public, is **non-newsworthy**.

Finley v. Kelly (M.D. Tenn 2019)

- Disclosure must be to the public at large.
- But some courts have held “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.”

Gill v. Hearst Publishing

Was the photograph disclosing private facts?
(Element 2)

*“It is significant that [the photograph] was not surreptitiously snapped on private grounds, but rather was taken of plaintiffs in a pose voluntarily assumed **in a public market place**”*

if in public, then not private



In re Facebook (N.D. Cal. 2019)

- Information shared with Facebook Friends is not inherently public, so there can be PDoPF liability for further sharing of it.
- “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.” Quoting the SC, in *Reporter’s Committee* (1989).

Newsworthiness and Republisher Immunity

Matthew Kugler

Privacy Law & Regulation

Shulman v. Group W Productions

Issue: Should the traumatic video have been aired?

- Yes, if a “logical nexus exist[s] between the complaining individual and the matter of legitimate public interest.”
- Strength of nexus vs. sensitivity of the disclosure

Y.G. v Jewish Hospital

- 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.

Sipple v. Chronicle Publishing

Issue: Should newspapers have been allowed to publish that Sipple was a gay man?

- Republisher Immunity: Had been published in obscure outlets. That is enough to make it public.
- Logical nexus: Connection between the private fact and the matter of public interest

Distributive consequences

- The same people will consistently find themselves to be “newsworthy.” Benefits and burdens accrue.
- Can be based on actions/choices. But also based on category membership, family connections, etc.

First Black Elected to Head Harvard's Law Review

By FOX BUTTERFIELD

Special to The New York Times

BOSTON, Feb. 5 — The Harvard Law Review, generally considered the most prestigious in the country, elected the first black president in its 104-year history today. The job is considered the highest student position at Harvard Law School.

The new president of the Review is Barack Obama, a 28-year-old graduate of Columbia University who spent four years heading a community development program for poor blacks on Chicago's South Side before enrolling in law school. His late father, Barack Obama, was a finance minister in Kenya and his mother, Ann Dunham, is an American anthropologist now doing fieldwork in Indonesia. Mr. Obama was born in Hawaii.

"The fact that I've been elected shows a lot of progress," Mr. Obama said today in an interview. "It's encouraging."

"But it's important that stories like mine aren't used to say that everything is O.K. for blacks. You have to remember that for every one of me, there are hundreds or thousands of black students with at least equal talent who don't get a chance," he said, alluding to poverty or growing up in a drug environment.



overwhelm this individual student's achievement."

Mr. Obama was elected after a meeting of the review's 80 editors that convened Sunday and lasted until early this morning, a participant said.

Until the 1970's the editors were picked on the basis of grades, and the president of the Law Review was the student with the highest academic rank. Among these were Elliot L. Richardson, the former Attorney General, and Irwin Griswold, a dean of the Harvard Law School and Solicitor General under Presidents Lyndon B. Johnson and Richard M. Nixon.

That system came under attack in the 1970's and was replaced by a program in which about half the editors are chosen for their grades and the other half are chosen by fellow students after a special writing competition. The new system, disputed when it began, was meant to help insure that minority students became editors of The Law Review.

Harvard, like a number of other top law schools, no longer ranks its law students for any purpose including a guide to recruiters.

Blacks at Harvard: New High

Black enrollment at Harvard Law School, after a dip in the mid-1980's, has reached a record high this year.

Michigan Law student becomes first Black Editor-in-Chief of 116-year-old Law Review

Sunday, January 28, 2018 - 5:01pm



Second-year Law student Megan Brown has spent the past seven years at the University, first for her undergraduate education and now for Law School. Buy this photo (<http://store.pub.umich.edu/michigan-daily-buy-this-photo/>)

Joshua Han/Daily

SAYALI AMIN (AUTHOR/TRAINING)

Daily Staff Reporter

Second-year Law student Megan Brown has spent the past seven years at the University, first for her undergraduate education and now for Law School.

Now, she has been selected as the editor in chief of the Michigan Law Review – a University of Michigan publication written by legal scholars, practitioners and students. She also discovered she would be the first Black person to hold this position at the Law Review, which issued its first publication in 1902.

She initially held the position of an associate editor of the Law Review, which she achieved after a rigorous process involving writing a paper, various publication-related exercises and interviews.

Brown said she felt honored to be chosen as editor in chief and attributed her success to those around her.

First Amendment and Public Disclosure

Matthew Kugler

Privacy Law & Regulation

First Amendment and Privacy

The publication of truthful private facts may be punished if:

- 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.

First Amendment and Privacy

The publication of truthful private facts may be punished if:

- 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**.

Cox Broadcasting v. Cohn / Florida Star v. B.J.F.

- Can media outlets be punished for publishing the names of rape victims when they get those names from the government itself?
- **No. Not least restrictive means. Government should be more careful.**

First Amendment and Privacy

The publication of truthful private facts may be punished if:

- 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.

Cox Broadcasting v. Cohn

- Family privacy: the dead cannot bring these kinds of privacy cases.
- **Solution: Father of deceased victim brings case for violation of his/family privacy.**

First Amendment and Privacy

The publication of truthful private facts may be punished if:

- 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.

Bartnicki v. Vopper

- Can the media be punished for publishing illegally obtained information if it was obtained without their involvement?
- **No, if the information is exceptionally newsworthy.**
- Balancing of First Amendment harms.

Government can punish people who disclose truthful information:

- ...that they lawfully obtained under an obligation of secrecy
 - Professional obligations, such as those of doctors and lawyers
 - Governmental employees and grand jurors.
- ...in breach of private contracts.
 - Nondisclosure agreements are enforceable absent public policy constraints.
- ...otherwise to further state interests of the highest order using the least restrictive means.

Defamation and Section 230

Matthew Kugler

Privacy Law & Regulation

Defamation

- **Elements:**
- A false and defamatory statement
- Unprivileged publication to a third party
- Fault (at least negligence) on the part of the publisher
- Harm

	Public Figure (includes Public Officials)	Private Figure
Speech of Public Concern	<i>Curtis</i> Compensatory Damages = Malice Punitive Damages = Malice Presume Damages = Malice	<i>Gertz</i> Compensatory Damages = Negligence Punitive Damages = Malice Presume Damages = Malice
Speech of Private Concern	Unclear Could be: 1. Same as above 2. <i>Gertz</i> rule 3. Malice for public official, <i>Gertz</i> for public figure	<i>Dun</i> Compensatory Damages = Negligence Punitive Damages = Negligence Presume Damages = Negligence (or possibly strict liability for all forms of damages)

Section 230 of the CDA

- “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.”
 - Communications Decency Act

ECPA and Online Monitoring

Matthew Kugler

Privacy Law & Regulation

Electronic Communications Privacy Act (ECPA)

- Wiretap Act: Governs live interception of “any wire, oral, or electronic communication.”
- Stored Communications Act: Governs access to electronic storage of communications.
- Pen Register Act: Governs live interception of noncontent information.

Wiretap Act

- "Wire" communications are made through the use of wire and include the human voice. (telephone call).
- An "oral" communication is one spoken by a person *who has a legitimate expectation that the communication will not be intercepted*.
- An "electronic" communication is a transfer of electronic data that is not either of the others (think email).

Wiretap Act General provision

- Unlawful to intercept the contents of a wire, oral, or electronic communication through the use of any electronic mechanical, or other device.
- Exceptions for
 - Interception needed to provide the service
 - Hearing aids
 - Broad transmission (think radio, social media)
 - Appropriate warrants
 - Consent of one party

Stored Communications Act (SCA)

- Cannot “intentionally access, without authorization, a facility through which an electronic communications service is provided, or to intentionally exceed the authorization for accessing that facility”

SCA Scope

- If you remotely store electronic files, you are probably a Remote Computing Service
- If you serve as an electronic communications platform, you are probably an Electronic Communications Service
- If you are just a website you aren't inherently either. And even if you are one you may not be one for the purposes of a particular person or set of data

Providers under SCA

- Providers of an electronic communication service to the public shall not knowingly divulge the contents of a communication while in electronic storage by that service
- Providers of a remote computing service to the public shall not knowingly divulge the contents of any communication which is carried or maintained on that service

Providers under SCA

- Host of exceptions for government legal process.
- Exception for consent.
- But: A provider may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications...
 - “to any person other than a governmental entity”

Consent and the ECPA

- Consent is a complete defense to monitoring under the ECPA.
- But consent needs to be explicit. Due to the sensitivity of live communication, courts generally unwilling to read into ambiguous language.

Types of Enforcement

- **Individual lawsuits:** Just you, usually small dollar figures unless something truly terrible happened. (Example: Intrusion upon seclusion).
- **Class action:** Lawsuit by you and everyone in the same position. (Example: Data breach).
- **Class action with statutory damages:** Same as above, but you don't need to prove extent of harm. Can get set damages even for minor violations. (Example: ECPA, FCRA).
- **Agency action:** You complain to a federal agency. They may fine the company, but they'll set the priorities. (Example: HIPAA)



Northwestern

Workplace Privacy

Matthew Kugler

Privacy Law & Regulation

Workplace monitoring

- Why do it?
 - Keep employees on task/not getting distracted.
 - Prevent theft by employees.
 - Control unprofessional behavior in workplace.
 - Identify good and problem employees.
 - Track workplace resources (room usage)

Workplace monitoring

- Risks:
 - Annoys employees.
 - Can cause employers to become aware of things that they would rather not know.
 - Antidiscrimination concerns
 - Union activity

Private Employers

- No uniform federal or state statute on this question.
- Can bring the basic privacy torts.
- Can bring statutory causes of action (Wiretap Act) when relevant.
- Can sue under discrimination or disability law (beyond our scope).

State laws on specific topics

These can vary state to state.

- Video monitoring is sometimes prohibited by statute in areas like bathrooms or changing rooms.
 - A few states require notice of cameras for employees.
 - Can always try to bring an Intrusion Upon Seclusion action as well.
 - Don't forget the Wiretap Act for audio monitoring
- Most video monitoring is unregulated, however.

State laws on specific topics

These can vary state to state.

- GPS monitoring of employee driving:
 - Generally legal even without employee consent in company-owned vehicles. Need consent for employee-owned.
 - Wording of these laws varies a great deal.
 - Likely to see issues with wearable devices in the future.

Workplace electronic searches

- Generally, office information technology workers log a lot of workplace computer activity.
- Regularly used in employment law cases (to justify firings) and trade secret cases.
- Generally permissible with notice and consent (defeats wiretap and intrusion upon seclusion claims).

Medical Confidentiality

Matthew Kugler

Privacy Law & Regulation

Duty of Confidentiality

- Elements:
 - Information conveyed to a physician, acting as physician, relevant to the treatment, under circumstances where confidentiality expected.
 - Unlawful disclosure.
- How is this different than Public Disclosure of Private Facts?

But...

- “various Vermont statutes compel medical providers to disclose certain information to protect the public.”
 - Gunshot wounds
 - Reports of disease associated with WMD
 - BAC of car accident patients
 - Various highly infectious/dangerous diseases
- Duty of confidentiality exists, but has exceptions.

Lawson v. Halpern-Reiss, 210 Vt. 224 (2019)

HIPAA regulation permits “disclosures to avert a serious threat to health or safety.” 45 C.F.R. § 164.512(j). Restricted to “serious and imminent threat.”

Here:

- Disclosure that a drunk person was about to drive is plainly averting a serious and imminent threat.
- Disclosure that she had driven is permissible given assumption of good faith. No evidence rebutting.

Recognized Evidentiary Privileges

- Vary by state.
- Widely recognized:
 - Attorney client privilege, spousal privilege (can refuse to testify), spousal privilege marital comm (can prevent from testifying), doctor-patient privilege (most states, not federal).
- Not widely recognized:
 - Parent-child, siblings, best friends, bartenders.

Jaffee v. Redmond, 518 U.S. 1 (1996)

- Establishes psychotherapist privilege. Officer Redmond's therapist cannot testify re the contents of her sessions.
- Stevens: Prevents chilling effect.

Take home on privilege

- Psychotherapist patient privilege is recognized in every state, with some nuance.
- Physician patient privilege is not as common and has more exceptions. Some states do not have it at all in criminal cases.

Tarasoff v Regents of Uni. of Ca.

- Poddar tells therapist Moore that he will kill Tatiana when she returns from Brazil.
 - Moore with agreement of two other doctors orders him committed.
 - Police pick him up and, convinced he is rational, release him.
- Poddar moves into an apartment with Tatiana's brother.
- Poddar kills Tatiana when she returns from Brazil.

HIPAA: Key Features

Matthew Kugler

Privacy Law & Regulation

HIPAA

Health Insurance Portability and Accountability Act

Coverage Scope

- Applies to entities that store records in HIPAA's "standard format." If you take insurance or file through any of the federal programs, you almost certainly do that. Otherwise, no.
- Associated businesses, insurance companies, etc. are equally regulated. Contracts through health care provider.

Protected Health Information (PHI)

- all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- There are no restrictions on the use or disclosure of de-identified health information.
 - Deidentification is hard.

Features of HIPAA

- Minimization when sharing information.
 - Does not apply to disclosures for treatment.
- Need to accommodate communication preferences (what can be left in a message).
- Data breach rules.
- Consent as key for all optional disclosures.
 - Marketing.

Common Misunderstandings

- Doctors refusing to give you your own medical records.
- Doctors thinking they cannot leave voicemails or send appointment reminder postcards.
- Doctors refusing to share information with family members.
- Doctors' offices refusing to ID waiting room thieves

Disclosures without consent

- Law enforcement use (with limits)
- Threats to health and safety
 - See *Lawson*
- To public health authorities
- To FDA regard adverse events
- To employers for on the job injuries

Shepherd v. Costco, 250 Ariz. 511 (2021)

- Shepherd is prescribed an ED medication but does not want to fill the prescription.
- Costco receives the prescription and fills it. Is repeatedly told to cancel it but doesn't.
- When Shepherd's estranged wife is asked to pick up his prescription for something else, she is also given the ED prescription. She ends efforts at reconciliation and further shares the information.

Shepherd v. Costco, 250 Ariz. 511 (2021)

- HIPAA does not include a private right of action, but it does permit more protective state law/additional enforcement mechanisms.
- Informs standard of care.
- Arizona law protects medical providers from good-faith errors in disclosing medical information, so remanded to a lower court to address that defense.

HIPAA: Enforcement

Matthew Kugler

Privacy Law & Regulation

Enforcement

- **No private right of action.**
- HHS has enforcement and fining authority
- Very few fines pre 2009 (pre Obama and pre HITECH Act).
- About 1,000 data breaches in five years.

Security Rule

- 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.
 - Training!

Data Breach Rule

- Breach is unauthorized “acquisition, access, use, or disclosure” of PHI.
 - Encrypted PHI is by definition not breached.
 - Lower risk unauthorized disclosures or uses may not be breaches
- Must notify affected individuals “without delay” (< 60 days).
- Report to HHS and notify local media if over 500 people.

Premiera Blue Cross Resolution Agreement (2020)

- Hack of PBC exposed ePHI of over 10 million people.
- Access gained via phishing/malware installation. Undetected for 8 months.
- Required to conduct Risk Analysis. Submit to HHS for approval.
- Create Risk Management plan based on the analysis. Implement.
- \$6.85 million fine.

Yakima Valley Memorial Hospital Press Release (2023)

- Security guards at hospital access the medical records of 419 individuals. Use their own legitimate login credentials.
- Emphasis on need for training in resolution.
- Fine of \$240,000

Civil enforcement, in general

- Focus on systematic failures of process rather than individual failings.
- If an individual failing appears, greater focus on why it was possible than why a bad actor did it.
- Employees as part of the problem.

Civil Stats

- Between 2018 and 2021:
 - 71.4% of complaints were resolved at the intake and review
 - 23.8% resulted in technical assistance to the accused party.
 - 2.0% were found not to be violations
 - 2.8% received corrective action.
- 53 monetary settlements from 2018-2021

Criminal Sanctions

- A person who knowingly:
 - Uses or causes to be used a unique health identifier;
 - Obtains individually identifiable health information....;
 - Or discloses individually identifiable health information....
- A person can be employee or other.

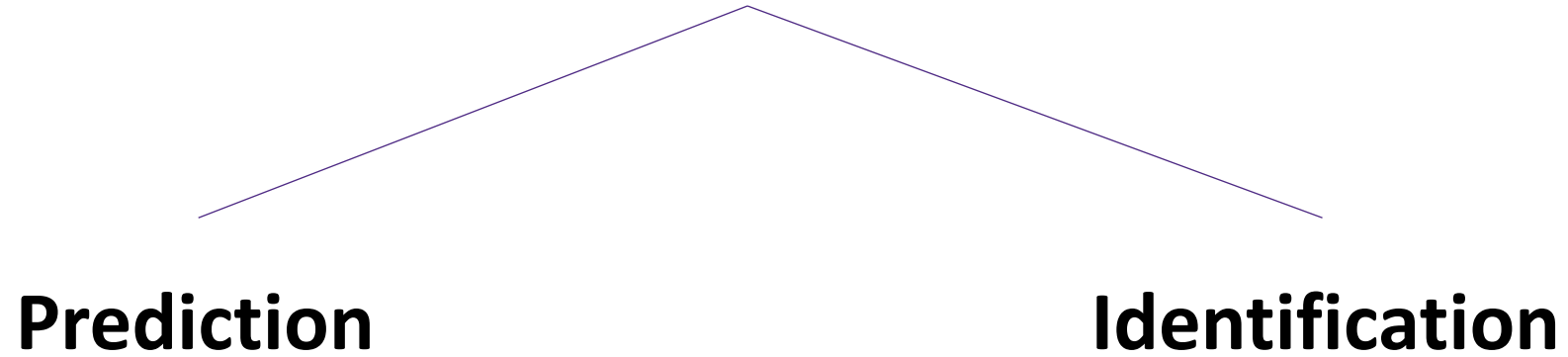
Northwestern

Genetic Privacy

Matthew Kugler

Privacy Law & Regulation

Genetic Privacy

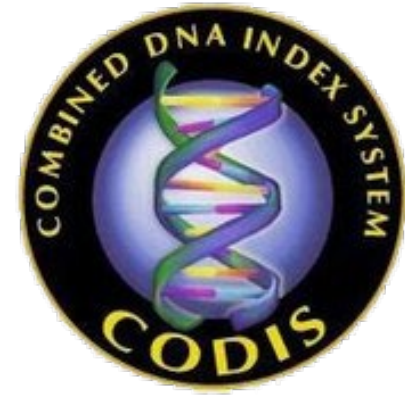


Prediction

Identification

Identification and DNA Databases

- Major DNA database is CODIS
 - Federal level.
 - 20 core loci (previously 13). Not enough information for prediction or family associations.
 - Database doesn't have names. Some protection against breach.
 - Database limited to LE collections.

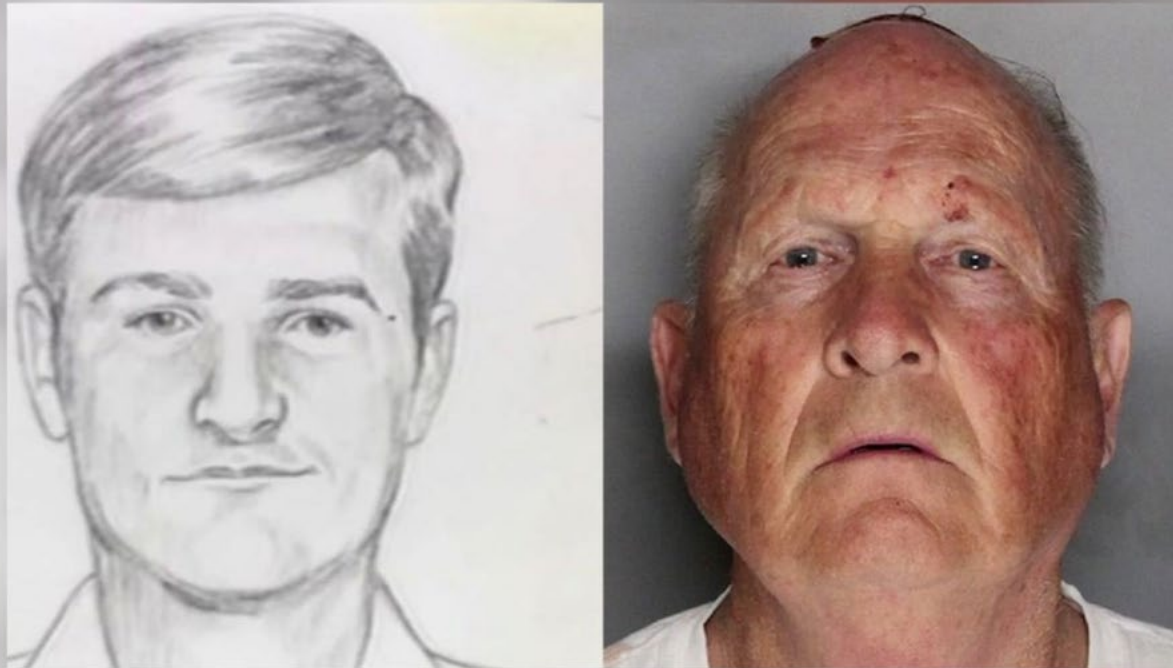


Maryland v. King, 569 U.S. 435 (2013)

- Involved use of swab DNA collection from arrestees. Only usable for identification.
- “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.”

GOLDEN STATE KILLER

DNA that cracked 'Golden State Killer' case came from genealogy websites



The suspected "Golden State Killer" Joseph James DeAngelo appears in this mugshot from Wednesday, April 25, 2018. (KGO-TV)



Welcome to you™

saliva collection kit



Future Diary and Prediction

- Hard question: Why is DNA special? Is this different than any other risk factor?
 - Unchosen
 - Immutable
 - Uncertain

Genetic Information Nondiscrimination Act (GINA, 2008)

- Bars discrimination in health insurance issuance and pricing based on genetic testing.
 - But not life insurance.
- Bars discrimination in hiring based on genetic testing. Also bars employer from requesting, requiring, or purchasing genetic information.

Data Brokers and Financial Privacy

Matthew Kugler

Privacy Law & Regulation

3,495,616 views | Feb 16, 2012, 11:02am

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did



Kashmir Hill Forbes Staff

Welcome to The Not-So Private Parts where technology & privacy collide

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. [Target](#) TGT +4.92%, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.



Target has got you in its aim

Privacy Torts and Consumer Data

- Dwyer v. American Express
 - Cardholders are classified into groups based on their buying habits, such as Rodeo Drive Chic or Value Oriented.
 - AmEx then sells lists of customers who fit particular profiles to merchants. Also offer to put together lists of customers interested in certain types of products, such as fine jewelry.

Dwyer v American Express

- Is this information private?
 - Voluntarily and necessarily disclosed.
 - Like magazine subscription lists.
- Is this a major problem?

Gramm Leach Bliley Act (GLBA)

- Applies to nonpublic personal information held by financial institutions.
- Cannot disclose account numbers for use in direct marketing.
- Must have annual privacy notice
- Must have data security

Gramm Leach Bliley Act (GLBA)

- Explicitly allows sharing of information with “affiliate” financial companies. Do not need permission or specific disclosure. Consumers can’t prevent.
- Can share with non affiliate companies
 - if consumers are given a chance to opt out, or
 - the nonaffiliate performs services for the financial institution, including marketing the financial institution’s own products.
- Only .5% exercise their opt-out rights. Only 41% recall receiving privacy notice.

The Fair Credit Reporting Act

Matthew Kugler

Privacy Law & Regulation

Fair Credit Reporting Act

- A “consumer reporting agency” (CRA) is any person who for remuneration “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.”
- A “consumer report” is any communication by a CRA “bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living.”
 - Must be used to establish eligibility for credit, insurance, employment, or other uses defined by FCRA.

11/14/2018

Report is Waiting

Building Report: Matthew

Please Confirm

— 2 — 3 — 4



There are limits to how you may use BeenVerified reports.
Please review the box below to continue to sign up.

- ☐ I will not use information provided by BeenVerified for decisions about employment, insurance, tenant screening, consumer credit or any other purpose restricted by the Fair Credit Reporting Act (FCRA) (<https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf>) . If you have any questions, view our Do's & Don'ts (<https://www.beenverified.com/about/dos-donts/>) page.

I AGREE

Fair Credit Reporting Act

- Within application, many consumer protections.
 - Need to “maintain reasonable procedures to limit the furnishing of consumer reports for enumerated ‘permissible purposes.’”
 - Must implement “reasonable procedures to assure maximum possible accuracy.”
 - Notice to consumers when reports used! Get consent for employment reports, share reports with consumer if take adverse action.
 - Barred from giving consumer reports to “persons that it did not have reason to believe had a permissible purpose to obtain a consumer report.”

Generally unregulated

- Marketing drawing on spending habits, magazine subscriptions, etc.

Regulated by FCRA

- Info brokered by "consumer reporting agencies"
- **Data used for credit, insurance employment, or other specified purposes**

Data Breach Notification and Litigation

Matthew Kugler

Privacy Law & Regulation

Data Breach Statutes

- All states have data breach notification statutes
- All require notification to the affected person.
 - Some on mere acquisition of information, some only if probability of misuse.
- More sophisticated states require notification to the state attorney general or state agency for large breaches (CA, IL, NY, VA etc.)
- Few have a private right of action (AK, CA, MD, MA, NC, WA). Some others allow under common law.

Some states: Require Risk of Misuse

- Michigan:
 - Notification is not required if the Entity determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of MI.

California's Law

- What is Personal Information (PI)?
 - Individual's name plus any of a list of elements:
 - Government ID numbers
 - Account or credit card number
 - Medical or health insurance information
 - Biometric data
 - Access tools for online account
 - E.g. Username or email + password. Security questions
 - (Provided that the information is unencrypted)

California's Law

- Applies to person, business, or state agency
- An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI.
 - Good-faith accidental acquisition by an employee of the entity does not count if the information is not further disclosed.

California's Law

- Notify if unencrypted information is, or is reasonably believed to have been, acquired by an unauthorized person.
 - Or if encryption key is obtained.
- Notify: affected person (can be by electronic notice), state AG if >500 CA residents.
- Timing: without unreasonable delay, consistent with law enforcement needs and internal security

California's Law

- Notification has specific requirements:
 - Dates when breach occurred. General description of incident. Contact information for company.
 - Specific headings (“What happened,” “What information was involved,” “What we are doing” etc.)
 - Offer of free identity theft protection if source of breach.

California's Law

- Requirement that companies use “reasonable security procedures”
- Private right of action – but no statutory damages.

Tsao v Captiva (11th Cir. 2021)

- Tsao was a customer at PDQ, a restaurant. PDQ had a data breach exposing payment information.
- Hack began May 2017, ran through April 2018. Tsao made two purchases in that time using credit cards.
- Upon learning of breach, cancelled his cards.

Tsao v Captiva (11th Cir. 2021)

- Alleged harms:
 - Increased risk of future identity theft.
 - But no actual 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.

Tsao v Captiva (11th Cir. 2021)

- “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.”
 - "elevated risk of identity theft" usually not enough by itself. Not even when SSN compromised (Reilly).

Tsao v Captiva (11th Cir. 2021)

- No standing on increased risk of future identity theft.
- No standing for minor incidental costs.
- What would Tsao's recovery have been even if he had standing?
Presumably minor.

Types of Harm in Data Breaches

- Emotion distress.
- Increased risk of future harm/ID theft.
- Precautions to reduce future harm.
- Liability for fraudulent charges.
- “Sorting out” costs.

In re Equifax

- Absolutely massive breach. 150 million people's data exposed.
- Some had suffered ID theft, so not like *Tsao*.
- Key issues:
 - What is the legal basis of the suit? Many causes of action across many different states.
 - What harm did Equifax cause? How will it be established that Equifax is liable for this person's suffering as opposed to that?

Problem of Broad Harms

- If 100,000 people have their data stolen in a breach, perhaps 3000-4000 will have their information used.
 - Most will not experience real financial loss.
 - But large collective harm (100,000 new credit cards, thousands of reversed retail transactions).
-
- How good is private litigation at resolving this?

The Federal Trade Commission as Privacy Enforcer

Matthew Kugler

Privacy Law & Regulation

Sectoral Approach vs. FTC

- Most privacy statutes are regulating only a particular technology, particular practice, or particular sector.
- This sector by sector approach is called a “sectoral” approach. Makes the edges of the regulation very important.
- The Federal Trade Commission has power that crosses sectors.

Federal Trade Commission (FTC)

- Federal agency charged with some aspects of consumer protection.
- Relatively small, budget of 430 million
- Historically concerned with antitrust and consumer fraud.
- Encouraged to work in privacy and data security starting in 1990s.

FTC's Section 5 Authority

- Section 5: “unfair or deceptive acts or practices in or affecting commerce.”
- Does not cover:
 - **Nonprofits**
 - Airlines
 - Many financial institutions
 - Telecom

FTC Deceptive Acts

- “A **deceptive** act or practice is:
 - a **material representation**, omission or practice
 - that is **likely to mislead** the consumer **acting reasonably** in the circumstances,
 - to the consumer’s **detriment**.”

FTC remedies

- No private right of action
- Can get injunctions under S5, but not issue fines except for violations of injunctions.
- So all injunctions bar further unfair acts or practices...giving them fining authority on round 2.
 - 20 years of monitoring.

In re Facebook (2019)

- Misrep. Extent to which users could limit sharing with 3rd party apps.
 - Affected friend data (data from friends of those using apps)
- Opt out rather than opt in for Facial Recognition, despite claims
- Failure to implement and maintain reasonable privacy program.

In re Facebook (2019)

- \$5B fine (\$70B annual revenue).
- New privacy board w/ more independence.
- Individual liability for desig. corp officers if they deceive FTC.
- Require 3rd party apps to self-certify compliance
- “affirmative express consent” to repurposing facial recognition.
- Data security.

FTC Unfair Acts

- An act is **unfair** if it:
 - “caused or is likely to cause **substantial injury** to consumers
 - which is **not reasonably avoidable** by consumers themselves
 - and is **not outweighed by countervailing benefits** to consumers or competition.”

Children's Privacy and COPPA

Matthew Kugler

Privacy Law & Regulation

COPPA

- Applies to an operator of a website or online service that is either
 - directed at children, or
 - has actual knowledge that it is gathering personal information from children under the age of 13.
- Such operators must get verifiable parental consent before collecting, using, or disclosing personal information obtained from children.
- Personal information:
 - anything identifiable, including screen names and email addresses. Physical location at street level. Photo or voice.
 - Persistent identifiers (IP address) are sufficient

Collection

- Need “verified” parental consent to collect information from <13.
 - Host of extremely limited exceptions.
- Collection can be asking for information, making it possible to provide the information in a profile, or passively gathering (cookies).
- Can’t condition games or prizes on information collection.

Directed at Children Factors

- whether the business's subject matter appeals to that age group
- whether the business offers visual and audio content aimed at young children
- the use of cartoon or animated characters
- the age of models used in advertisements
- the use of child celebrities or celebrities that are favored by children

US v Youtube (2019)

- YouTube toymakers that “YouTube is today’s leader in reaching children age 6-11 against top TV channels” and that YouTube is the “#1 website regularly visited by kids.”
- Several channel owners told YouTube that their channels were directed to children
 - YouTube’s own content rating system identified content as directed to children
- 170 million dollar fine, require channels to self-designate as child-directed.

3rd Party Liability

- 16 CFR § 312.2, a third party “[w]eb site 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 Web site or online service directed to children.”
- Ad network getting information from child directed website?
- Website with child directed content contributed by a 3rd party?

The Federal Trade Commission and Data Security

Matthew Kugler

Privacy Law & Regulation

FTC Unfair Acts

An act or practice is unfair where it:

- “caused or is likely to cause **substantial injury** to consumers
- which **is not reasonably avoidable** by consumers themselves
- and is **not outweighed by countervailing benefits** to consumers or competition.”

FTC Data Security Guidelines – Main Themes

- Limit the information you collect to what you actually need
- Limit who in your organization can access each piece of sensitive information to what they need.
- Control access to your network, especially external access.
- Basic tech hygiene: Use firewalls, keep your software up to date, and change default passwords.
- Employ two-factor authentication.
- Train your employees both to resist phishing schemes and to avoid misusing data.

FTC v. Wyndham

- Wyndham Worldwide suffers repeated data breaches. FTC brings suit.
- 10.6 million in fraud losses from 600k sets of data (~\$16 per)
- Wyndham argues:
 - the Section 5 unfairness authority does not extend to data security; and
 - the FTC has failed to give fair notice of what data security practices are required by law.

Where did Wyndham Fail?

- Stored payment card information in clear readable text.
- Allowed the use of easily guessed passwords to access the property management systems..
- Failed to use firewalls
- Allowed remote access to central systems without insisting on decent security from the contacting networks.
 - Same, with third party vendors
- Poor anti-intrusion detection or post-incident investigation.

A company cannot be compelled to adopt “*a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers [and] shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity [etc].*”

- LabMD, Inc. v. Federal Trade Commission (2018)
- **Need more precise orders going forward.**

And we got them. Equifax, 2019 required:

- Requiring confirmation that any directives to apply patches or remediate vulnerabilities are received and completed ...;
- Designing and implementing protections such as network intrusion protection, host intrusion protection, and file integrity monitoring...;
- 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, such as multi-factor authentication and strong password requirements;
- Limiting user access privileges to systems that provide access to Personal Information to employees ... 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...

Recent Data Security Enforcement Actions

- Chegg (2022). Four Breaches from 2017-2022.
 - Multiple Chegg employees fell for a phishing attack that allowed a hacker to gain access to employees' direct deposit information.
 - Former contractor used login information the company shared with employees and outside contractors to access one of Chegg's third-party cloud databases containing personal information of approximately 40 million customers.
 - Two more phishing attacks exposed sensitive data about Chegg's employees including medical and financial information.

Going forward

- Common FTC targets are companies that have repeated or egregious failures of security. Either multiple hacks or exceedingly large hacks.
- Will always ask for about the same things. Usual problems are employee failures (phishing), poor network security/segmentation, or both.
- Severely resource constrained. Cannot bring more than a few of these actions in a year.