UC Irvine Law Review

Volume 10 | Issue 1 Article 5

10-2019

From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms

Matthew B. Kugler

Follow this and additional works at: https://scholarship.law.uci.edu/ucilr

 Part of the Law Commons

Recommended Citation
Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 U.C. IRVINE L. REV. 107 (2019).
Available at: https://scholarship.law.uci.edu/ucilr/vol10/iss1/5

This Article is brought to you for free and open access by UCI Law Scholarly Commons. It has been accepted for inclusion in UC Irvine Law Review by an authorized editor of UCI Law Scholarly Commons.

From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms

Matthew B. Kugler*

Central to understanding biometric privacy is the question of biometric privacy harms. How much do people value biometric privacy, and what evils should biometric privacy laws seek to avert? This Article addresses these questions by surveying two nationally representative samples to determine what does, and does not, worry people in the context of biometrics. The results show that many people are deeply concerned about biometric privacy in the consumer context, that they are willing to sacrifice real benefits to preserve biometric privacy, and that those who are concerned with biometric privacy attribute their concern to many factors that are not directly related to data security, particularly public tracking. Further, people's level of comfort with biometric data collection differs sharply depending on the uses to which the data will be put and not just on the type of data collected. These nuanced attitudes about biometric privacy are in sharp conflict with a purely data security approach to biometric harms, and therefore have substantial implications both for future legislative consideration as well as current standing litigation.

* Associate Professor, Northwestern University Pritzker School of Law. The author thanks Jane Bambauer, Anne Boustead, Erin Delaney, Shari Diamond, Eric Goldman, Janice Nadler, Jim Pfander, David Schwartz, Nadav Shoked, Matthew Spitzer, and Lior Strahilevitz for comments on earlier drafts, as well as Myriam Bloom, Eva Derzic, and Alexander Ogren for helpful research assistance.

INTRODUCTION

Issues of biometric privacy have arisen with increasing frequency over the last several years as biometric scanners have become cheaper and more prevalent.[1] Though advocates have been sounding the alarm about biometric privacy for decades, by 2018 even Microsoft was calling for greater regulation of facial recognition technology.[2] Along with this increased concern 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.[3] In the trenches of the Northern District of California, for example, Facebook is facing more than $30 billion in potential liability for violations of biometric privacy laws.[4]

---

1. 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).

2. Drew Harwell, *Microsoft Calls for Regulation of Facial Recognition, Saying It's Too Risky to Leave to Tech Industry Alone*, WASH. POST, (July 13, 2018), https://www.washingtonpost.com/technology/2018/07/13/microsoft-calls-regulation-facial-recognition-saying-its-too-risky-leave-tech-industry-alone/ [http://web.archive.org/web/20190702174455/https://www.washingtonpost.com/technology/2018/07/13/microsoft-calls-regulation-facial-recognition-saying-its-too-risky-leave-tech-industry-alone/] (reporting company president Brad Smith's statement: "This technology can catalog your photos, help reunite families or potentially be misused and abused by private companies and public authorities alike. The only way to regulate this broad use is for the government to do so.").

3. *See, e.g.*, Steven Grimes & Eric Shinabarger, *Biometric Privacy Litigation: The Next Class Action Battleground*, BLOOMBERG LAW: BIG LAW BUS. (Jan. 17, 2018), https://biglawbusiness.com/biometric-privacy-litigation-the-next-class-action-battleground [https://perma.cc/F4BU-VRGQ] (noting that over 60 class action lawsuits have been filed under BIPA since 2015); Scott Holland, *Judge: No 'Risk of Harm' to Rexnord Workers from Fingerprint Scan Time Clocks; Case Sent Back to Cook Courts*, COOK COUNTY REC. (July 20, 2018), https://cookcountyrecord.com/stories/511494676-judge-no-risk-of-harm-to-rexnord-workers-from-fingerprint-scan-time-clocks-case-sent-back-to-cook-courts [https://perma.cc/HZ2S-EHZV] (discussing lawsuit against Rexnord Industries for use of fingerprint-based timeclock system); Anna S. Knight & Patrick J. Castle, *Employers Face a Rise in Biometric Privacy Suits*, WORKFORCE (Feb. 7, 2018), https://www.workforce.com/2018/02/07/employers-face-rise-biometric-privacy-lawsuits/ [https://perma.cc/6W8Z-LKA3] (suggesting that the "recent spate" of BIPA litigation is not an anomaly but indicative of more litigation to come).

4. Class Action Complaint, Pezen v. Facebook, No. 1:15-cv-03484 (N.D. Ill. Apr. 21, 2015); Consol. Class Action Complaint, Licata v. Facebook, Inc., No. 3:15-cv-03747-JD (N.D. Cal. Aug. 28, 2015); *see also* 740 ILL. COMP. STAT. 14/15, 20 (2019). For damage figures, see calculations in Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. S69, S95 n.2 (2016). Thus far, Facebook has been unable to have the case dismissed at the district court level and the Ninth Circuit recently upheld class certification on interlocutory appeal. Patel v. Facebook, Inc., No. 18-15982, 2019 WL 3727424, at *7 (9th Cir. Aug. 8, 2019).

The Facebook litigation is only part of a wave of lawsuits filed under Illinois law against companies for the improper collection and use of biometric data. Some of these suits have been filed against major technology companies due to their helpful—perhaps too helpful—analysis of user-uploaded photos.[5] More lawsuits have been filed against companies that use fingerprint readers and other biometrics to clock employees in and out during shift changes.[6] Such biometric timekeeping technologies have been increasingly used in recent years as companies have sought to avoid the "buddy punch" problem of workers being marked as present by friends.[7] In January of 2019, the Illinois Supreme Court upheld a broad interpretation of its state privacy law, making it likely that such litigation will continue for the foreseeable future.[8]

Despite this rash of attention to biometrics, we know precious little about how everyday people view uses of biometric technology and why they might value biometric privacy. Many courts have adopted the view that biometric privacy serves only to protect against identity theft.[9] Under this limited perspective, it poses little problem when companies begin to collect large amounts of biometric data.[10] These courts, therefore, see no harm and find no standing to sue.[11]

But consider how three alternate rationales for protecting biometric privacy affect the harm analysis—the analysis which determines whether these lawsuits are even permitted in federal court. If one believes that the point of a biometric privacy law is to protect against identity theft, then one is not harmed by biometric data collection until the possibility of such theft has increased. This is a data security

---

5. *See, e.g.*, Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1090 (N.D. Ill. 2017); Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

6. *See, e.g.*, McGinnis v. United States Cold Storage, Inc., No. 17 C 08054, 2019 WL 95154, at *1 (N.D. Ill. Jan. 3, 2019); Goings v. UGN, Inc., No. 17-CV-9340, 2018 WL 2966970, at *1 (N.D. Ill. June 13, 2018); Howe v. Speedway LLC, No. 17-CV-07303, 2018 WL 2445541, at *1 (N.D. Ill. May 31, 2018).

7. *See, e.g.*, Becky Yerak, *Companies Sued Over Use of Biometric Data*, CHI. TRIB., http://digitaledition.chicagotribune.com/tribune/article_popover.aspx?guid=25cf7766-b719-4140-91d7-e0657dec6a36 [https://perma.cc/KK93-6EBZ] (last visited Aug. 11, 2018) (reporting on lawsuits filed by employees contesting fingerprint-based timeclocks); *Eliminate Punching With our Biometric Solutions*, TREERING (Mar. 25, 2018), https://treeringws.com/eliminate-buddy-punching-with-our-biometric-solutions/ [https://perma.cc/V344-G377] (explaining biometric buddy punching solution); *What Is Buddy Punching and How to Prevent It*, TSHEETS, https://www.tsheets.com/resources/prevent-buddy-punching [https://perma.cc/3PKG-Z2BM] (last visited Aug. 11, 2018) (explaining buddy punching and estimating damages caused by buddy punching to employers).

8. *See* Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186 ¶34 (Jan. 25, 2019); *see also* Ben Kochman, *Users Say Ill. Ruling Should Halt Facebook Face ID Appeal*, LAW360 (Feb. 1, 2019), https://www.law360.com/articles/1124568/users-say-ill-ruling-should-halt-facebook-face-id-appeal [https://perma.cc/QK7L-NNUF] (discussing the impact of the decision on pending litigation).

9. For examples of these court decisions, see *infra* note 20.

10. For a discussion of biometric security, see *infra* notes 103–103 and accompanying text.

11. For examples of these court decisions, see *infra* note 20.

justification for protecting biometric privacy, and it would likely require little regulation. Many cases will therefore be dismissed if this is the only rationale for protecting biometric privacy. If one is concerned about the possibility of tracking people in public using facial recognition, however, then the data security conversation is beside the point—even perfect security against the outside world is of little use if the company that collected and owns the data is allowed to use it as it likes. This concern is addressed only by use and collection restrictions and would require extensive regulation. Further, if one believes that the collection of biometric information represents a dignitary affront, then harm occurs at the moment of unauthorized information acquisition even if no further actions are taken. This set of harms can only be addressed by outright bans or strong notice and consent requirements. Again, this could justify intrusive regulation and would lead courts to find harm in a wide range of cases.

These various concerns are not mutually exclusive; one could be uneasy with biometric information collection for many reasons. These concerns also may not be entirely distinct; one could view biometric collection as a dignitary affront because of the practical implications for public tracking rather than for abstract or philosophical reasons. Nevertheless, it is useful to distinguish between these potential "whys." Particularly, it is very important to know whether we should be thinking only in terms of data security when we are contemplating harms or whether we should take a broader approach.

One purpose of this Article is to evaluate which of these rationales speaks to Americans' concerns. Privacy law has often looked to public norms to understand the extent and nature of privacy rights. In their seminal article, *The Right of Privacy*, Samuel Warren and Louis Brandeis grounded their call for greater legal protection of privacy in law's recognition "of man's spiritual nature, of his feelings and his intellect."[12] Similarly, the Supreme Court has referenced public understandings when considering who can give consent to searches of shared private spaces[13] and in evaluating whether a location or an item counts as private at all.[14] Finally, there is

12. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193, 213 (1890); *see also id.* at 195 ("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 invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer.").

13. Georgia v. Randolph, 547 U.S. 103, 111 (2006) ("The constant element in assessing Fourth Amendment reasonableness in the consent cases, then, is the great significance given to widely shared social expectations.").

14. *See, e.g.*, Bond v. United States, 529 U.S. 334, 338–39 (2000) ("When a bus passenger places a bag in an overhead bin, he expects that other passengers or bus employees may move it for one reason or another. Thus, a bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner."); Minnesota v. Olson, 495 U.S. 91, 98 (1990) ("To hold that an overnight guest has a legitimate expectation of privacy in his host's home merely recognizes the everyday expectations of privacy that we all share. Staying overnight in another's home is a longstanding social custom that serves functions recognized as valuable by society."); California v. Carney, 471 U.S. 386, 392 (1985) ("The public is fully aware that it is accorded less privacy in its automobiles because of this compelling governmental need for regulation. Historically, 'individuals always [have] been on notice that movable vessels may be

a growing movement in Fourth Amendment scholarship to make the extent of privacy protections partially contingent on popular expectations.[15]

The stakes in the biometric privacy domain are high, making the question especially urgent. Statutory damages under the Illinois statute start at $1000 per negligent violation and go to $5000 for intentional or reckless violations.[16] National technology companies are therefore changing their behavior in response to this law,[17] and lobbying over new biometric legislation has been fierce.[18] And many of the best anti-privacy arguments, both in the courtroom and the statehouse, all turn on harm. Is your face really private given that you show it so readily to people you meet? What are you afraid is going to happen?

This Article seeks to address these questions using data collected from two nationally representative surveys. Why, and how much, do people care about biometric privacy? Are people uniquely concerned about the collection of biometric information, or is such data no different than the dozens of other data trails that we leave streaming behind us in daily life? Would people be willing to pay fees or forgo benefits to protect their biometric information? What reasons would they give for doing so? How much do people distinguish between different kinds of biometric technologies? Is it a problem if biometrics are collected with the understanding that they will be used in one way, and they are instead used in another?

The data presented here show that people are concerned about the collection of biometric information, even when it is presented in mundane, matter-of-fact contexts. They report that they are willing to forgo benefits to avoid the collection of biometric information, and that they would be willing to pay more for services to protect biometric privacy.

Those participants who reported being uncomfortable with biometric data collection said that their discomfort stems from many concerns rather than just one. Though most participants were concerned about data security and identity theft, supermajorities also cited other issues. People said they felt it was invasive for a

---

stopped and searched on facts giving rise to probable cause that the vehicle contains contraband, without the protection afforded by a magistrate's prior evaluation of those facts.'") (internal citations omitted).

15. *See, e.g.*, Bernard Chao, Catherine S. Durso, Ian P. Farrell & Christopher T. Robertson, *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 Cal. L. Rev. 263 (2018); Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 259 (2016); 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, 52–53 (2015); 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); Alisa Smith, Sean Madden & Robert P. Barton, *An Empirical Examination of Societal Expectations of Privacy in the Digital Age of GPS, Cell Phone Towers, and Drones*, 26 ALB. L.J. SCI. & TECH. 111, 133 (2016); Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 177 (2016).

16. 740 Ill. Comp. Stat. 14/20 (2019).

17. *See infra* notes 4–56 and accompanying text.

18. *See infra* note 99 and accompanying text.

company to collect their biometric data, that the possibility of being publicly tracked using their biometrics bothered them, and that they were worried where the collection of biometric information could lead in the future.

People also distinguish sharply between different uses of biometric technology. A second data collection, in Part IV, asked participants to report how comfortable they were with eighteen different biometric uses. When the biometric information was being used for a limited purpose closely related to security—be it to lock a smartphone or scan a store for known bad actors—most people were fairly comfortable with the technology. For example, 71% said they were comfortable with using a fingerprint to unlock a smartphone, and 59% approved of the store-scanning. When the technology was being used for broad scale public tracking, however, people were much less comfortable. Fully 74% were *uncomfortable* with a store using facial recognition to track consumer shopping behavior. In general, modest majorities were comfortable with the use of biometrics in the place of passwords and large majorities were *uncomfortable* with more adventurous uses of biometrics. So even if people were willing to have their biometric data used in one way, they were often resistant to some other uses. And a minority was uncomfortable for each possible use.

All these findings speak to the question of biometric privacy harm and, in general, these data support taking a broad view of what counts as harm. The meaning of harm is a subject of recurring dispute in privacy litigation, where it is central to issues of both standing and remedies.[19] Specifically, in the domain of biometric privacy, we have seen issues of harm litigated in two separate contexts. The first is in disputes over standing: when has a party been harmed such that they can sue?[20] This is a threshold issue that arises in both federal and state courts.[21] At

19. Matthew S. DeLuca, *The Hunt for Privacy Harms After Spokeo*, 86 FORDHAM L. REV. 2439, 2457–66 (2018) (reviewing standing in recent privacy suits); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 748 (2018) (noting that "harm drives the way courts think about data-breach cases").

20. *Compare* Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 15 (2d Cir. 2017) ("We further conclude, pursuant to the second step of our inquiry, that none of the alleged procedural violations here raise a material risk of harm to this interest."), *and* Howe v. Speedway LLC, No. 17-CV-07303, 2018 WL 2445541, at *7 (N.D. Ill. May 31, 2018) ("Defendants undoubtedly violated BIPA if [they committed procedural violations]. However, those procedural violations did not cause him an injury-in-fact."), *with* Patel v. Facebook, Inc., No. 18-15982, 2019 WL 3727424, at *6 (9th Cir. Aug. 8, 2019) ("By contrast, Facebook's alleged collection, use, and storage of plaintiffs' face templates here is the very substantive harm targeted by BIPA. Because we conclude that BIPA protects the plaintiffs' concrete privacy interests and violations of the procedures in BIPA actually harm or pose a material risk of harm to those privacy interests, the plaintiffs have alleged a concrete and particularized harm, sufficient to confer Article III standing.") (internal citations omitted), *and* Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *8 n.5 (N.D. Ill. Sept. 15, 2017) (finding federal jurisdiction and declining to dismiss).

21. *See, e.g.*, federal cases cited *supra* note 20; state cases such as Greer v. Ill. Hous. Dev. Auth., 122 Ill. 2d 462, 492–93 (1988).

the close of this Article, we shall examine in detail how the study results should inform the standing analysis in these ongoing cases.[22]

The second context in which this question arose was the interpretation of the Illinois Biometric Information Privacy Act (BIPA), under which much of the current litigation has been filed. This statute provides a private right of action to "aggrieved" parties.[23] Defendants had generally argued that only data security-style harms are concrete enough to make a person "aggrieved," with plaintiffs naturally replying that even minor violations of the notice and consent provisions of the statute are sufficient.[24] The Illinois Supreme Court recently resolved this statutory question in favor of the plaintiffs' interpretation, holding that violations of the statute's notice and consent provisions are not "merely" technical.[25] "When a private entity fails to adhere to the statutory procedures . . . '[T]he right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.'"[26]

In taking this view, the Illinois Supreme Court adopted an explicitly broad view of the kinds of rights that biometric privacy legislation can legitimately seek to protect—it treated control of biometric information as an inherent good.[27] Many of the federal courts receiving these cases have taken a narrower view.[28] Going forward, we will continue to see this question litigated in a variety of contexts. Perhaps most importantly, each state will have to answer it as they seek to draft their own privacy legislation. In Massachusetts, for instance, the state legislature is currently considering a bill that would codify the same broad understanding of biometric rights that is now the law in Illinois.[29]

Part I of this Article begins by reviewing the ways in which biometric technology is currently being used and the kinds of protections provided by current

---

22. *See infra* Part IV.C.

23. 740 ILL. COMP. STAT. 14/20 (2019). According to the primary architect of the statute, this terminology was borrowed from the Illinois Civil Rights Act of 2003. 740 ILL. COMP. STAT. 23 (2019).

24. *See, e.g.*, Order re Class Certification at 9–10, *In re* Facebook Biometric Info. Privacy Litig., No. 3:15-CV-03747-JD, 2018 WL 1794295, at *6 (N.D. Cal. Apr. 16, 2018) ("Facebook contends that [the] issue[] can only be resolved by individual evidence of . . . whether a class member is 'aggrieved' as that word is used in BIPA . . . ."); Rosenbach v. Six Flags Entm't Corp., No. 16-CG-13, 2017 WL 6523910, at *2 (Ill. App. Ct. Dec. 21, 2017), *perm. app. granted*, 98 N.E.3d 36 (Ill. 2018) (summarizing defendants' argument that plaintiff had no standing because she failed to allege any actual injury).

25. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 34.

26. *Id.* (quoting Patel v. Facebook Inc., 290 F. Supp. 3d 948, 953 (N.D. Cal. 2018)).

27. *Id.*

28. *See, e.g.*, Aguilar v. Rexnord LLC, No. 17-CV-9019, 2018 WL 3239715, at *3 (N.D. Ill. July 3, 2018) ("A person's privacy may be invaded if her biometric information is obtained or disclosed without her consent or knowledge . . . . But notice and consent violations do not without more create a risk of disclosure."); *see also supra* note 20.

29. Nadia Dreid, *Mass. Bill Would Make Clandestine Data Harvesting An Injury*, LAW360 (Jan. 31, 2019), https://www.law360.com/articles/1123807/mass-bill-would-make-clandestine-data-harvesting-an-injury [https://perma.cc/6B8S-C8Q4] ("Under the proposed bill, individuals wouldn't have to show how they had been injured by a company's gathering of their data - the fact that it had been collected at all without their consent would be considered an injury itself.").

state privacy laws. Part II presents data from a nationally representative survey that seeks to answer the question of whether people value biometric privacy, and whether they are willing to make sacrifices to preserve it. Part III considers the various rationales that have been advanced for protecting biometric privacy and tests how they relate to the public's stated motivations in that same study. Part IV presents a second study that considers how the public feels about a wide range of different uses of biometric technology. Finally, Part V reviews the implications of these results both from the standpoint of privacy theory and in terms of the concrete question of Article III standing.

I. BIOMETRIC PRIVACY PROTECTIONS

Biometric identification is becoming ubiquitous in society. Many employers make their employees clock into and out of work using fingerprints rather than timecards.[30] Banks and other financial institutions use biometrics of all sorts for an extra level of security[31] and now so do some educational testing centers.[32] Airlines have considered using facial recognition to verify passenger identities at check-in.[33] Retail stores use facial recognition to track suspected shoplifters,[34] and some

30. For an example of claims stemming from the use of this type of time-keeping technology, see Dixon v. Washington & Jane Smith Cmty.—Beverly, No. 17 C 8033, 2018 WL 2445292, at *1 (N.D. Ill. May 31, 2018) (BIPA claim for employer's mandate that employees clock in and out of work by scanning fingerprints onto Kronos biometric timekeeping device). For details of the product, see *Kronos InTouch Timeclock*, KRONOS, https://www.kronos.com/products/kronos-intouch [https://perma.cc/X6NX-RVYR] (last visited Sept. 5, 2019).

31. *E.g.*, VANGUARD, ACCESS YOUR ACCOUNT BY PHONE SECURELY AND CONVENIENTLY USING VANGUARD VOICE VERIFICATION (2011), HTTPS://PERSONAL.VANGUARD.COM/PDF/C106.PDF?2210065141 [https://perma.cc/2RT5-H29C]; *see also* Lisa Jane McGuire, *Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving up Your Privacy*, 33 AKRON L. REV. 441, 443–45 (2000); *From Fingerprints to Faces: Bank of America Explores Biometrics' Next Phase*, PYMNTS.COM (Sept. 27, 2017), https://www.pymnts.com/news/security-and-risk/2017/bank-of-america-biometrics-facial-recogniton/ [https://perma.cc/DA2Q-5689].

32. Lauraann Wood, *Test Cos. Face Ill. Biometric Lawsuits Over Finger, Vein Scans*, LAW360 (July 10, 2018), https://www.law360.com/articles/1061573/test-cos-face-ill-biometric-lawsuits-over-finger-vein-scans [https://perma.cc/6X7A-UUXJ].

33. Mark Albert, *Airport Biometrics Expand: Bag Drop, Check-in, Lounge Access, Boarding*, VOYAGE REP. (June 1, 2017), https://www.voyagereport.com/news/airport-biometrics-expand/ [https://perma.cc/4BFQ-A6KF]; Hugo Martin, *JetBlue and Delta Begin Testing Biometrics to Identify Passengers*, L.A. TIMES (June 1, 2017), https://www.latimes.com/business/la-fi-airline-biometrics-20170601-story.html [https://perma.cc/3S54-WBUE]; Benjamin Zhang, *Delta Wants to Use Facial Recognition Technology to Make Checking Your Bags Easier*, BUS. INSIDER (May 15, 2017), https://www.businessinsider.com/delta-facial-recognition-software-check-bag-lines-2017-5 [https://perma.cc/WR6V-YNWW].

34. *Lowe's U.S. Privacy Statement*, LOWE'S, (ver. effective Nov. 20, 2017, available at https://perma.cc/U6M9-4AMR) ("In some stores, we may use facial recognition technologies to identify known shoplifters. Specifically, we may use specialized cameras to scan the faces of persons entering the facility and create a unique set of data points. These data points are compared—in real time—against data points of faces of shoplifters who have previously agreed in writing that they will no longer be allowed in our stores. The scan data is retained only if we identify a biometric match to our database of known shoplifters. Otherwise, the scan data is immediately deleted. We do not use facial recognition or other biometric identifiers for marketing purposes or to build profiles of shoppers." Based on

companies are reportedly using it to track all shoppers in their stores.[35] Walgreens is now piloting a line of "smart coolers" that use facial analysis to detect the sex and approximate age of those who open them.[36] Companies are even marketing biometric identification to churches and schools as a means of tracking attendance and participation.[37] Perhaps most famously, Apple has allowed people to use their fingerprints to unlock their phones for years, and it added a facial recognition option for their latest phone model in 2017.[38]

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,[39] and it is also using facial recognition to identify jaywalkers and red-light runners.[40] Though some might be concerned merely by the automated detection and punishment of petty crimes, there is a further issue specific to the Chinese context. China's government-run "social credit system" rewards and punishes citizens based on characteristics such as honesty, norm-following, and general courtesy,[41] and it appears that biometric tracking is being used to further increase the system's accuracy.[42] This

information saved on web.archive.org, this language appears to have been removed from the live version of the privacy policy on July 27, 2018).

35. Annie Lin, *Facial Recognition Is Tracking Customers As They Shop in Stores, Tech Company Says*, CNBC (Nov. 23, 2017), https://www.cnbc.com/2017/11/23/facial-recognition-is-tracking-customers-as-they-shop-in-stores-tech-company-says.html [https://perma.cc/8QJN-YAEU].

36. *See* Sidney Fussell, *Now Your Groceries See You, Too*, ATLANTIC (Jan. 25, 2019), https://www.theatlantic.com/technology/archive/2019/01/walgreens-tests-new-smart-coolers/581248/ [https://perma.cc/8UTD-66KG].

37. *See Church Management*, BAYOMETRIC, http://www.bayometric.co.uk/biometric-church-management/ [https://perma.cc/D4KJ-CRXT] (last visited Aug. 11, 2018); IDENTIMETRICS INC., THE GROWTH OF BIOMETRICS IN SCHOOLS (2017), available at https://www.identimetrics.net/images/Growth-of-Biometrics-in-Schools.pdf [https://perma.cc/5Y96-U4U4].

38. In September 2017, Apple Inc. launched an iPhone that users can unlock with their face. *The Future is Here: iPhone X*, APPLE: NEWSROOM (Sept. 12, 2017), https://www.apple.com/newsroom/2017/09/the-future-is-here-iphone-x/ [https://perma.cc/LL4B-PX5A].

39. *See* Stanley Lubman, *The Unprecedented Reach of China's Surveillance State*, CHINA FILE (Sept. 15, 2017), http://www.chinafile.com/reporting-opinion/viewpoint/unprecedented-reach-of-chinas-surveillance-state [https://perma.cc/ASX6-7KUM].

40. *See* Dake Kang, *Chinese 'Gait Recognition' Tech IDs People by How They Walk*, ASSOCIATED PRESS (Nov. 6, 2018), https://www.apnews.com/bf75dd1c26c947b7826d270a16e2658a [https://perma.cc/E8GJ-JBDK] ("Chinese police are using facial recognition to identify people in crowds and nab jaywalkers, and are developing an integrated national system of surveillance camera data."); Renlian Shibie Xitong Luxu Jiuwei Chuanghongdeng Jiangnaru Chengxin Zhidu (人脸识别系统陆续就位 闯红灯将纳入诚信 制度) [*With Facial Recognition Systems Eventually in Place Jaywalking Will Be Entered into Credit Record*], SOHU 搜狐 [SOHU] (Mar. 24, 2018), http://www.sohu.com/a/226282563_351146 [https://perma.cc/Y26U-9VNA] (describing how facial recognition systems allow for the tracking of jaywalking).

41. Xin Dai, Toward a Reputation State: The Social Credit System Project of China 14 (June 10, 2018) (unpublished manuscript) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193577 [https://perma.cc/ATC5-G4AY]) (describing the scope of the term "shehui xinyong" and the applications of the system). The author is indebted to Dai's translation of the Sohu source, cited in the preceding footnote.

42. *Id.* at 32, 47–50, 59 (commenting on both the applications of biometrics and the authoritarian objectives the system allows the government to pursue).

Chinese facial recognition technology has already been exported to other countries and was successfully deployed in Brazil for Carnival in 2019, resulting in several arrests.[43] Though such extensive use is not currently being considered in the United States, facial recognition technology is on the rise even here. For example, a major producer of police body cameras is already considering the ethical implications of introducing facial recognition to their products.[44]

Regardless of a system's ultimate purpose, most biometrics are used in the same two ways: they either identify or authenticate an individual.[45] Upon enrollment in a biometric system, a person's biometric identifier is scanned and converted into a digital code. When that person is later scanned again, the results of the later scan can be compared to those of the earlier scan to determine whether there is a match.[46] This can be done to either confirm an identity of an individual—"Is this Jane, the owner of the account?"—or to identify an unknown person by comparing the 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.[47]

As of the beginning of 2018, only Illinois, Washington, and Texas had biometric privacy laws.[48] California passed a broad privacy law that includes protection for biometric data that summer and this law will take effect in 2020.[49]

---

43. *See* Fernanda Távora, *Gabrielle Araújo and Jordan Sousa, Scanner facial abre alas e ninguém mais se perde no Carnaval (e fora dele)* [*Facial Scanner Debuts and Nobody Else Gets Lost in Carnival (and Out of It)*], TAB (Mar. 3, 2019), https://tab.uol.com.br/noticias/redacao/2019/03/11/carnaval-abre-alas-para-o-escaner-facial-reconhece-milhoes-e-prende-seis.htm [https://perma.cc/M8AC-LGNE] (describing the Brazilian use of the technology and several of those arrested); Helton Simões Gomes, *Reconhecimento facial usado na China é testado no Brasil; saiba como opera* [*Facial Recognition Used in China Is Tested in Brazil; Learn How It Works*], UOL (Jan. 18, 2019), https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/01/18/reconhecimento-facial-usado-na-china-e-testado-no-brasil-saiba-como-opera.htm [https://perma.cc/6V95-X6RZ] (describing a legislative fact-finding trip to China to investigate expanded use of Chinese facial recognition technology).

44. Dana Goodyear, *Can the Manufacturer of Tasers Provide the Answer to Police Abuse?*, NEW YORKER (Aug. 27, 2018), https://www.newyorker.com/magazine/2018/08/27/can-the-manufacturer-of-tasers-provide-the-answer-to-police-abuse [https://perma.cc/F3JB-K27V].

45. April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/ [https://perma.cc/GCX9-GVMZ] (defining biometric technology as "technology that does one of two things: identifies you or authenticates your identity").

46. Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1390–91 (2004); McGuire, *supra* note 31, at 444–45; John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns – Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 100 (1997).

47. Daniel J. Steinbock, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 FLA. L. REV. 697, 704–05 (2004).

48. 740 ILL. COMP. STAT. 14/15 (2019); TEX. BUS. & COM. CODE ANN. § 503.001 (2019); WASH. REV. CODE § 19.375.010 (2019); *see also* Sharon Roberg-Perez, *The Future Is Now: Biometric Information and Data Privacy*, 30 ANTITRUST 60, 62–63 (2017) (describing the then-current state of efforts to pass legislation in other states).

49. CAL. CIV. CODE § 1798.100 (2019).

The exact definition of biometric information varies state by state. In Illinois, under whose Biometric Information Privacy Act (BIPA) all the current litigation has been filed, "biometric identifier" is defined to include "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[50] Several types of information are specifically excluded from the category of biometric identifiers in Illinois, including basic demographic information; physical descriptors such as height, weight, and eye color; photographs; and most information collected from patients in a healthcare setting.[51] The definition under Washington State's law is similar but specifically excludes information generated from photographs and videos, such as the facial geometry data collected by Facebook from uploaded user photos.[52]

The protections offered by different state laws vary meaningfully. In Illinois, for example, a private entity cannot collect biometric information unless it provides a written privacy policy to the person whose information is being collected.[53] This policy must contain some very specific disclosures about the purpose of the collection and the ways in which the biometric data will be secured. The entity also must obtain written consent from the person.[54] These notice and consent requirements form the basis of every case under BIPA of which the author is aware.

In general, this set of requirements can be satisfied with appropriately drafted privacy policies and consent procedures. If one uses biometric timekeeping for one's employees, an additional form at the time of hiring and some greater attention to data security may be all that is required. But compliance is not so easy in other contexts. For example, a NEST home security camera equipped with facial recognition is programmed to not activate that feature in Illinois; one simply cannot get consent from everyone who might approach one's security cameras so the product cannot legally be used.[55] Similarly, in Illinois and Texas, Google disabled a feature in their Arts and Culture app that allowed people to see what great works of art resemble them, presumably over concerns that people would upload photographs of others and therefore cause Google to be in violation of state laws if it generated biometric scans of these non-consenting individuals.[56] Even a cute

50. 740 ILL. COMP. STAT. 14/10 (2019).

51. *Id.*

52. WASH. REV. CODE § 19.375.010 (2017).

53. 740 ILL. COMP. STAT. 14/10.

54. 740 ILL. COMP. STAT. 14/15(b)(3) (2019).

55. *See, e.g.*, Tess Townshend, *Nest's New Camera Uses the Same Facial Recognition Tech As Google Photos*, RECODE (May 31, 2017), https://www.recode.net/2017/5/31/15708124/nest-iq-camera-indoor-facial-recognition-technology-google-photos [https://perma.cc/4UPK-RJRU] (discussing release of $299 indoor camera with facial recognition software and decision not to make the technology available in Illinois).

56. *See, e.g.*, Ally Marotii, *Google's Art Selfies Aren't Available in Illinois. Here's Why*, CHI. TRIB. (Jan. 17, 2018), http://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html [https://perma.cc/V6TX-WNZ4].

robotic dog has been excluded from Illinois because it is able to distinguish between family members using facial recognition.[57]

Home security, arts apps, and robotic puppies aside, there is a further provision of BIPA that may be more consequential, at least in the long term, than the notice and consent requirements. This provision prohibits a private entity that possesses biometric information from selling, leasing, trading, or otherwise profiting from that biometric information.[58] It therefore outright bans certain kinds of commercial conduct rather than requiring informed consent. And these barred uses are not obscure. One could easily imagine a major technology company wanting to lease access to their facial recognition database to a major producer of CCTV cameras. Amazon's "Rekognition" service, which provides cheap storage and analysis of face data, could be a vehicle for such a use.[59] Amazon markets its service as being able to "perform real-time face searches against collections with tens of millions of faces," "detect, analyze, and index up to 100 faces . . . in a single image," and "analyze sentiments for all faces in group photos, crowded events, and public places such as airports and department stores."[60] In Illinois, many of the possible uses of this technology would simply be illegal for private actors.

This bar on profiting from the collection of biometrics is currently unique to Illinois.[61] The Illinois statute is also unique in another way: only it provides a private right of action.[62] The statutes in Washington and Texas can only be enforced by the state attorney general, and as best the author can determine, there have been no enforcement actions filed by those offices.[63] Much biometric enforcement in the United States therefore comes from private lawsuits filed on behalf of Illinois residents.

---

57. *See, e.g.*, Neil Steinberg, *Want This Cute Robot Dog? Tough — Illinois Law Keeps Sony from Selling It Here*, CHI. SUN TIMES (Nov. 15, 2018), https://chicago.suntimes.com/business/sony-robot-dog-aibo-biometrics-illinois-supreme-court-lawsuits-informed-consent-abt-electronics/ [https://perma.cc/MEM5-7PSN] (describing Sony's robot dog that uses facial recognition to identify different family members).

58. 740 ILL. COMP. STAT. 14/15(b).

59. *Amazon Rekognition*, AWS, https://aws.amazon.com/rekognition/ [https://perma.cc/7QTB-JDKY] (last visited Aug. 11, 2018). Microsoft offers a similar service called "Face API." *See Face,* MICROSOFT AZURE, https://azure.microsoft.com/en-us/services/cognitive-services/face/ [https://perma.cc/SPQ5-YPY6] (last visited Aug. 11, 2018).

60. Ranju Das, *Amazon Rekognition Announces Real-Time Face Recognition, Support for Recognition of Text in Image, and Improved Face Detection*, AWS MACHINE LEARNING BLOG (Nov. 21, 2017), https://aws.amazon.com/blogs/machine-learning/amazon-rekognition-announces-real-time-face-recognition-support-for-recognition-of-text-in-image-and-improved-face-detection/ [https://perma.cc/T48X-5KZC].

61. *See* Elvy, *supra* note 1, at 495 (discussing this difference).

62. 740 ILL. COMP. STAT. 14/20 ("Any person aggrieved by a violation of this Act shall have a right of action . . . against an offending party.").

63. TEX. BUS. & COM. CODE ANN. § 503.001(d) ("The attorney general may bring an action to recover the civil penalty."); WASH. REV. CODE ANN. § 19.375.030 (2019) ("This chapter may be enforced solely by the attorney general . . . .").

This brings us to the question that motivates this Article: why? Four states have taken at least some action to protect biometric privacy, and bills are being considered in several others. What, if anything, is so scary about biometric information? Several alternate theories have been advanced. Before addressing those, however, we should not discount the possibility that there is absolutely nothing special about biometrics. Your fingerprint geometry may not be widely known, but it also exposes virtually no personal information. From a mere fingerprint, you cannot deduce character, habits, or relationships. Fingerprints are also surrendered regularly to the government and to some employers, and certainly few people take great pains to avoid leaving them behind in a restaurant. A fingerprint is therefore neither revealing nor overly secret.

One might say a face is different, with facial recognition allowing for tracking in public. But faces are different in the anti-privacy sense as well: it is a rare person who does not regularly show their face to all whom they pass on the street.[64] Thinking about the ease with which people turn over images of their faces—both on social media and by merely appearing in public—it is hard to argue that facial geometry is truly private.

The possibility that biometric information may simply not be private prompts the question of how much people value biometric privacy. Are people made less comfortable by information collection merely because the collection happens by means of biometrics or includes biometrics data? Are they willing to sacrifice some benefit, or incur some cost, to keep biometric data private? These are the questions that Part II seeks to answer.

II. DO PEOPLE VALUE BIOMETRIC PRIVACY?

There are many reasons why people might care about biometric privacy, but there is little data indicating how much they do or why they do. The purpose of this study was to experimentally compare reactions to accomplishing a goal with and without using biometric technology. Specifically, participants were presented with realistic monitoring and tracking programs that either worked via biometric technologies or worked via ID cards. The primary question was whether people were less comfortable with the biometric tracking technologies and whether they would be willing to accept some cost, or forgo some benefit, if it allowed them to opt out of the biometric regime.

Though some researchers have conducted surveys on biometric privacy in the past, those surveys have tended to focus on particular subject areas rather than taking a broad approach. For example, a 2016 survey by Pew asked whether

64. Some proportion of Muslim women wear face-concealing clothing, but this is very rare in western countries. *See, e.g.*, Carol Kuruvilla, *Danish Muslim Women Protest as Ban on Face Veils Enters Full Force*, HUFFPOST (Aug. 1, 2018), https://www.huffpost.com/entry/danish-muslim-women-protest-as-ban-on-face-veils-enters-full-force_n_5b61ea77e4b0b15aba9f24b0 [https://perma.cc/KKV5-F7CE] (citing research estimating that only 150–200 women in Denmark choose to wear such).

participants would consider it acceptable to install a facial recognition-capable surveillance camera in a workplace that had experienced a number of employee thefts.[65] Fifty-four percent of those surveyed said yes, and twenty-four percent said no, but many of the comments made by participants focused on the particulars of 1) a workplace and 2) a place with a history of thefts.[66] It is hard to make sweeping claims about biometric privacy from such a focused question.

Other studies have considered use of biometrics in interactions that have traditionally been seen as high-security, such as banks.[67] And a survey by Accenture Federal Services asked about willingness to share certain kinds of biometric information with the government, again a special case.[68] Though these types of surveys have generally shown moderate to high levels of comfort with biometrics, there is some reason to think that people are more comfortable with biometrics in these security-conscious contexts than in the mass market.[69] The comfort reflected in these surveys is also not overly relevant to current litigation because government entities and most financial institutions are exempted under BIPA.[70] It appears that there is almost no research on the kinds of basic consumer uses of biometrics that have been the subject of most of the recent lawsuits. Also, an unfortunate proportion of the existing data is proprietary—meaning that the details of both the questions and the results are unavailable.

---

65. Lee Rainie & Maeve Duggan, *Privacy and Information Sharing: Many Americans Say They Might Provide Personal Information, Depending on the Deal Being Offered and How Much Risk They Face*, PEW RES. CTR. (2015), http://assets.pewresearch.org/wp-content/uploads/sites/14/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf [https://perma.cc/JM4P-4QET].

66. *Id.* at 15–16.

67. Most of these surveys are, sadly, not publicly available. Results from some of these surveys are discussed in a variety of places, however. *See* INT'L BIOMETRICS & IDENTITY ASS'N, RECENT OPINION SURVEYS ON PUBLIC PERCEPTIONS OF BIOMETRICS (Mar. 2016), https://www.ibia.org/download/datasets/3372%20/Public-Perceptions-of-Biometrics-opinion-surveys%20.pdf [https://perma.cc/V9R3-WP27]; Justin Lee, *Study Finds Americans Support Biometrics-Based Payment Systems*, BIOMETRICUPDATE.COM (July 18, 2018), https://www.biometricupdate.com/201707/study-finds-americans-support-biometrics-based-payment-systems [https://perma.cc/9VT6-N993].

68. *Majority Willing to Share Biometrics for Better eGovernment,* PLANETBIOMETRICS (Apr. 5, 2018), http://www.planetbiometrics.com/article-details/i/7002/desc/majority-willing-to-share-biometrics-for-better-egovernment/ [https://perma.cc/N5R6-PDVQ] (discussing results of survey regarding the willingness of individuals to share biometric data to improve government services).

69. *Study Explores Biometric Data as 'Currency' for Govt Services*, PLANETBIOMETRICS (Feb. 4, 2016), http://www.planetbiometrics.com/article-details/i/4109/desc/study-explores-biometric-data-as-currency-for-govt-services/ [https://perma.cc/KFS4-BFQD]; *see also Biometric Technology Enjoys Strong Support from Consumers, Says CTA*, BUS. WIRE (Mar. 30, 2016), https://www.businesswire.com/news/home/20160330006149/en/Biometric--Technology--Enjoys--Strong--Support--Consumers--CTA [https://perma.cc/TX5F-HZKR] (noting that "*More than half* of U.S. adults are [comfortable] with the use of biometrics in locations commonly believed to already have a high degree of security screening . . . . Also, *almost half* of consumers are comfortable using biometric technologies at home and/or the workplace.") (emphasis added). The report is sadly not publicly available. See also the data presented here in Part IV.

70. 740 ILL. COMP. STAT. 14/25 (2019).

One report by Rachel L. German and K. Suzanne Barber did consider privacy motives, however.[71] They asked those who reported being uncomfortable with biometrics to say why. The most common response (43.7%) was that biometrics were an invasion of personal privacy, with only 19.3% reporting concern with identity theft and 23.6% citing the possibility of government tracking.[72] These appear to have been exclusive options, however, so they do not shed light on the possibility that people might have multiple different reasons for being concerned. They also found that people by far had the most experience with fingerprint biometrics, that they largely used biometrics to log in to their personal devices and accounts, and that on a ranking question, they reported more comfort with fingerprint biometrics than with any other kind.[73]

None of these existing studies include the kind of experimental data collected here. This study considered three different consumer domains in which biometrics have been used.

A. Scenarios and Comfort Ratings

A sample of American adults was recruited by Research Now/SSI, an online survey firm with an established panel.[74] The demographics of the sample were set to match U.S. census proportions on the dimensions of age, sex, region, education, and race/ethnicity. Full demographics are reported in the Appendix. The final sample contained 1226 individuals.[75]

The purpose of this first study was to see how participants would respond to a rich description of biometric technology being used in a real-world context. Each participant in the study saw a single biometric privacy scenario from one of three domains: employee timekeeping, gym membership check-in, and a coffee shop loyalty program.

The employment vignette put participants in the role of an employee. It described how many employers had their employees check into and out of work

---

71. Rachel L. German & K. Suzanne Barber, *Consumer Attitudes About Biometric Authentication: A UT CID Report*, U. TEX. AUSTIN CTR. FOR IDENTITY (May 2018), https://identity.utexas.edu/assets/uploads/publications/Consumer-Attitudes-About-Biometrics.pdf [https://perma.cc/SX9Q-KY4Q].

72. *Id.* at 15. The authors also report high level of comfort with use of various types of biometrics. They do not include much information about the exact question they asked to generate this data, however, and repeated requests for further information have not been answered.

73. *Id.* at 5–6.

74. Research Now has since been absorbed by Dynata. *Announcing New Name and Brand: Research Now SSI Is Now Dynata*, DYNATA, (Aug. 8, 2019), https://www.dynata.com/press/announcing-new-name-and-brand-research-now-ssi-is-now-dynata/ [https://perma.cc/J29B-WMVX].

75. Inattentive participants were screened from the final sample based on two criteria. First, participants who did not give the appropriate response to either of two attention check questions—questions asking participants to give a particular response—were unable to complete the study. Second, participants were screened from the final sample if they finished the study in less than one-third of the time taken by the median participant.

and that, though this is more common among hourly employees, it is increasingly used for salaried employees as well. The description continued with a review of the check-in process. Upon arrival, the employee would scan either their ID card or, in the biometric condition, their thumbprint, at a machine by the company's main entrance. They would repeat the process upon departure.

The vignette then went on to describe the employer's data retention policy. All participants were told that the employer would keep the arrival and departure information indefinitely and could use it for any purpose. In the ID card condition, the policy stopped there. In the biometric conditions, the policy continued in one of two ways. Some biometric participants were told that the thumbprint information would be kept indefinitely and could be shared or sold. Other biometric participants were told that the information would be destroyed upon an employee's departure from the company and would never be shared or sold.

There was a further nuance to the biometric conditions. Some participants were given a full justification for biometric timekeeping: "The company began using thumbprints last year to avoid what it called the buddy punch problem. Some employees were having friends sign them in or out. The use of thumbprints ensures that people can only check themselves in and out." Others were only given the following seven words: "The company began using thumbprints last year." Many lawsuits under BIPA are about employers using fingerprint scanners to monitor their employees' arrivals and departures, so this vignette was well in line with the facts of actual cases.[76]

Here is the text of the thumbprint scenario in which the biometric data were not destroyed and no justification was given:

> Many employers require their employees to check in and out when they enter and leave work. This is particularly common for hourly employees, but is increasingly used for salaried employees as well. Imagine that you are working at a company that tracks its employees in this way. At the beginning of every shift, you scan your thumbprint at a machine by the company's main entrance. The machine compares the thumbprint with its database of employee thumbprints and marks you as having arrived. The process repeats at the end of the day as you scan out at a different machine. The employer keeps this arrival and departure data indefinitely and can use it for any purpose.
>
> The company also retains a record of the thumbprints for all current and former employees and keeps that information indefinitely. It never deletes the thumbprint information. It is free to use the information for any purpose, including sharing it or selling it.
>
> The company began using thumbprints last year.

76. For examples of these court decisions, see *infra* note 6.

There were five variants of this scenario: a 2 (thumbprint data destroyed or retained) x 2 (thumbprint use justified or not) design with a control condition (ID card). The control condition was oversampled such that it received one third of the total participant pool. A figure showing the list of variants for each scenario appears later in this Section.

After the scenario was presented, all participants were asked to answer two questions on 0-100 scales ranging from Very Uncomfortable to Very Comfortable. The first question asked how comfortable they were with the company's method of checking in at work. The second question asked how comfortable they were with the company's data retention policy. These two questions were used in each of the other scenario domains as well.

The other two scenario domains were checking in at a gym and using a loyalty rewards program at a coffee shop. These scenarios were fundamentally quite similar to each other. The gym scenario described how many gyms have members check in with a card or key fob. Participants were then told that their gym either used this same method or instead used either thumbprints or facial recognition.

For the gym vignette, there were again five variants: a keycard condition, two thumbprint conditions, and two facial recognition conditions.[77] The four conditions that included biometric information had the same privacy policy options as in the employment case. Participants were either told the biometric information would be destroyed when it was no longer needed and would never be shared, or that the information was the gym's to do with as it pleased. No justification information was provided.

Here is the facial recognition gym scenario in which the biometric information is being protected:

> Many gyms require their members to check in when they arrive. This is sometimes done by showing identification at a desk, but is increasingly automated by having people scan a card or keychain tag.
>
> Imagine that you are a member of a gym that tracks when members arrive using facial recognition. Upon arrival, you look directly at a scanner and it matches your facial geometry to your membership information. This is also how the gym's lockers work. Each locker is similarly equipped with a scanner.
>
> The gym retains a record of the arrival and departure times for all current and former members and keeps the information forever. It is free to use the information for any purpose and share or sell it.
>
> The gym retains a record of the facial recognition information of all current members, but deletes the facial recognition information within one month of their membership ending. The gym only uses the facial recognition information to track attendance and will never use the information for any other purpose or share or sell it.

77. In both the gym and coffee shop domains the control condition was again oversampled.

The gym vignette may seem somewhat fanciful at first glance, but there are two pending BIPA cases with similar facts. In *Sekura v. Krishna Schaumberg Tan*,[78] the plaintiff alleges that the defending salon used fingerprint biometrics to track her use of their services. And *McCollough v. Smarte Carte* concerns use of biometric lockers.[79]

The same types of conditions were used in the coffee shop vignette: card, thumbprint, or facial recognition, with biometric data either being protected or not. Here, the information was used to administer a customer loyalty program:

> Imagine that you regularly go to a coffee shop or restaurant that tracks when customers arrive using thumbprints. As you approach the register, you press your thumb onto a scanner and it matches your thumbprint to your customer information.
>
> This system lets the person at the register greet customers by name, suggest favorite orders, and track bonus discounts.

In all three of these sets of scenarios, the data privacy protection that sometimes applied to the biometric information was never extended to non-biometric information. In the coffee shop domain, for example, all participants were told, "The coffee shop retains a record of the order information for all current and former members of its customer loyalty program and keeps the information indefinitely. It is free to use the information for any purpose." This was done to ensure that any comfort derived from biometric information security policies was specific to biometric information and that participants would not assume that other customer information was similarly protected.[80] In the sample gym scenario above, you can note the same contrast between arrival and departure information (not protected in any condition) and facial recognition information (protected in that condition).

---

78. Sekura v. Krishna Schaumberg Tan, Inc., No. 1-18-0175, 2018 WL 4699213 (Ill. App. Ct. Sept. 28, 2018).

79. McCollough v. Smarte Carte, Inc., No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016).

80. The two biometric information protection policies that participants saw for the thumbprint conditions were:

The coffee shop also retains the thumbprint information of all current and former members of its customer loyalty program forever. It is also free to use the thumbprint information for any purpose and share or sell it.

OR

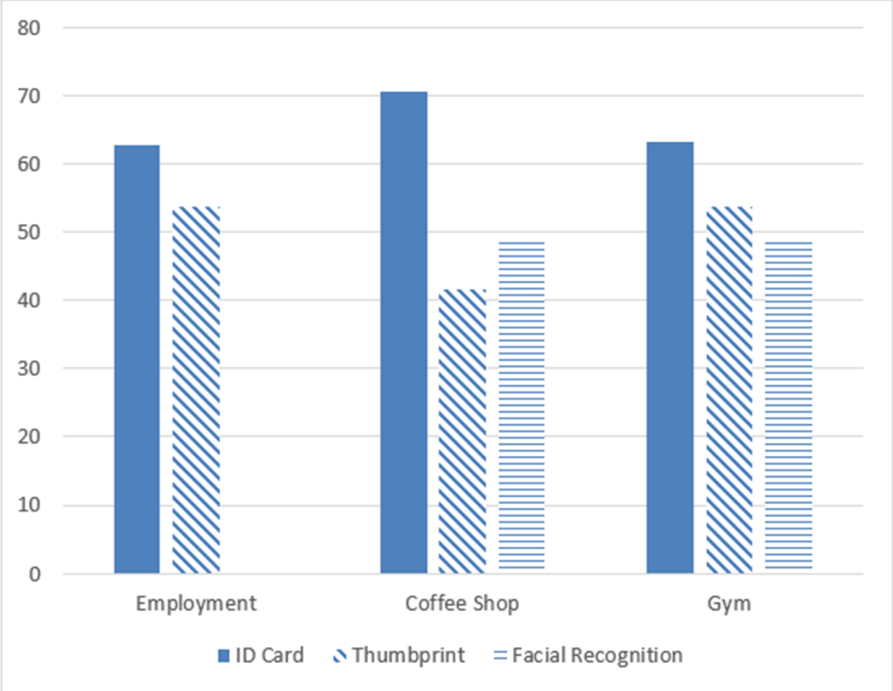
The coffee shop retains a record of the thumbprint information of all current members of its customer loyalty program but deletes a member's records within one month of them cancelling their membership or after a period of inactivity. The coffee shop only uses the thumbprint information to track customer orders and will never use the information for any other purpose or share it.

The below figure summarizes the various experimental conditions:

Employer	Gym	Coffee Shop
ID card	ID card	ID card
Thumb-Destroy-Justified	Thumb-Destroy	Thumb-Destroy
Thumb-Destroy-Not Justified	Thumb-Retain	Thumb-Retain
Thumb-Retain-Justified	Face-Destroy	Face-Destroy
Thumb-Retain-Not Justified	Face-Retain	Face-Retain

As can be seen in Table 1 and Figure 1, collecting biometric information substantially reduced comfort in each domain. For the employment domain, use of thumbprints made participants on average about 9 points less comfortable on the 101-point scale. For the gym context, it was 9.5 points. For the coffee shop, however, it was 28.8 points. When facial recognition information was used, it similarly made people less comfortable on average: 21.5 points lower than control in the coffee shop domain and 13.9 in the gym domain. Biometric tracking therefore was consistently a source of greater discomfort.

Figure 1: Estimated Comfort Levels by Type of ID Used



Note: Based on the regression reported in Table 1. The comfort dependent measure ranged from 0 to 100 with higher numbers indicating greater comfort. Estimated at Age = 35, Female = 0, Social Class and Education = 3.

Table 1: Standardized and unstandardized betas for regressions predicting comfort ratings in each domain.

	Employment (N = 402)				Coffee Shop (N = 404)				Gym (N = 417)			
	Check-in		Retention Policy		Check-in		Retention Policy		Check-in		Retention Policy	
	Unstand B.	Std Beta	Unstand B.	Std Beta	Unstand B.	Std Beta	Unstand B.	Std Beta	Unstand B.	Std Beta	Unstand B.	Std Beta
(Constant)	54.48 (6.89)		46.67 (6.90)		61.51 (6.53)		58.13 (6.75)		52.50 (6.97)		51.89 (7.00)	
Female	2.83 (3.18)	.04	4.70 (3.18)	.07	0.34 (3.06)	.01	-0.27 (3.16)	.00	0.04 (3.11)	.00	-1.46 (3.12)	-.02
Age	0.14 (0.09)	.08	0.09 (0.09)	.05	-0.13 (0.09)	-.07	**-0.23 (0.09)**	**-.12 ***	**-0.24 (0.09)**	**-.13 ****	**-0.33 (0.09)**	**-.17 *****
Education	-1.21 (1.54)	-.05	-2.06 (1.54)	-.07	-0.17 (1.54)	-.01	0.00 (1.59)	.00	1.20 (1.47)	.04	-0.80 (1.48)	-.03
Social Class	2.31 (1.93)	.07	**4.90 (1.94)**	**.14 ***	**4.70 (1.77)**	**.14 ****	**3.52 (1.83)**	**.11 +**	**5.15 (1.87)**	**.15 ****	**5.60 (1.88)**	**.16 ****
Hispanic	-1.48 (4.27)	-.02	2.08 (4.28)	.02	-3.49 (4.08)	-.04	-5.09 (4.21)	-.06	-6.62 (4.13)	-.08	-5.64 (4.15)	-.07
African Amer.	-4.08 (4.78)	-.04	-4.09 (4.79)	-.04	0.27 (4.61)	.00	0.68 (4.77)	.01	**12.97 (4.55)**	**.14 ****	**16.22 (4.56)**	**.17 *****
Thumbprint	**-9.01 (4.31)**	**-.14 ***	**-13.69 (4.32)**	**-.20 ****	**-28.81 (4.10)**	**-.42 *****	**-21.39 (4.24)**	**-.31 *****	**-9.50 (4.28)**	**-.14 ***	**-9.27 (4.29)**	**-.14 ***
Facial Rec.					**-21.52 (4.11)**	**-.32 *****	**-14.75 (4.25)**	**-.22 *****	**-13.85 (4.15)**	**-.20 *****	**-13.30 (4.17)**	**-.19 ****
Destroy	**15.97 (4.01)**	**.23 *****	**25.66 (4.02)**	**.35 *****	4.62 (3.68)	.07	**8.44 (3.81)**	**.12 ***	5.19 (3.72)	.08	**11.18 (3.73)**	**.17 ****
Justification	5.81 (4.04)	.09	1.78 (4.05)	.03								
R^2	.034		.117		.137		.093		.102		.118	

Note: *** p< .001; **p < .01; * p < .05; + p < .10. Standard errors are in parentheses. The comfort dependent measure ranged from 0 to 100 with higher numbers indicating greater comfort with either the check-in procedure or the data retention policy. Social class was measured on a scale with the following response options: Low Income (1), Working Class (2), Middle Class (3), Upper Middle Class (4), Upper Class (5). Education ranged from Less than High School (1); High School Diploma, GED, or equivalent (2); Some College Credits or Associate's Degree (AA, AS, etc.) (3); 4 Year College (BA, BS etc.) (4); Graduate or professional degree (5).

The employment vignette did not include a facial recognition variant and the coffee shop and gym vignettes did not include justification variants.

In something of a puzzle, the data protection provisions provided different levels of comfort across domains. In the employment context, having biometric information collected with a data security provision (marked "destroy" in Table 1) actually resulted in higher levels of comfort than not collecting biometrics at all. In the coffee and gym domains, this effect was smaller and only significant on the questions that specifically referenced the data retention policies.

The data reveal a few noteworthy demographic differences. First, those with higher self-reported social class are significantly more comfortable on four of the six measures, and the effect is in the same direction on the two measures for which it is not significant. This is a main effect on comfort with tracking and is not specific to any particular method of monitoring (keycard or biometrics), so it should be understood as a greater acceptance of monitoring for customer loyalty benefits and check-ins more generally. This effect was not anticipated.[81] One possibility is that those of higher social class get more benefits from these sorts of programs and are more accustomed to them. Anyone who has flown domestically is familiar with the kinds of benefits that can come with "status" on an airline, for instance, and such status comes at substantial cost. Another possibility is that those of lower class are more likely to have had negative experiences with these programs. Though some companies track the movements of employees of every level,[82] being penalized for being slightly late is likely more commonly the experience for hourly employees.

More surprising is the effect of age in the coffee shop and gym contexts. Several papers have shown that younger people have greater privacy expectations and place a higher value on many kinds of privacy.[83] Here, however, the young are slightly more comfortable than the old with these tracking programs, reversing that pattern. This effect appears to be present only in the two non-employment contexts—the gym and the coffee shop—and is non-significantly in the other direction for the employment measures. Again, we can only speculate about why this effect may be present. Perhaps younger people do not value privacy in this kind

81. A reanalysis of the expectations of privacy data collected by Matthew B. Kugler and Lior J. Strahilevitz did not reveal an independent effect of social class. Matthew B. Kugler & Lior Strahilevitz, *Assessing the Empirical Upside of Personalized Criminal Procedure*, 86 U. CHI. L. REV. (forthcoming 2019).

82. Kaveh Waddell, *Why Bosses Can Track Their Employees 24/7*, ATLANTIC (Jan. 6, 2017), https://www.theatlantic.com/technology/archive/2017/01/employer-gps-tracking/512294/ [https://perma.cc/M3UQ-ZZGY].

83. Bernard Chao, Ian Farrell, Catherine Durso & Christopher Robertson, *Why Courts Fail to Protect Privacy: Race, Age, Bias and Technology*, 106 CAL. L. REV. 263, 312–14 (2018) (showing that the middle aged had slightly higher privacy expectations against government surveillance than the young and much higher expectations than the old); Matthew B. Kugler & Lior J. Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 252–54 (2016) (showing that people with lower privacy expectations against a government search are older); Kugler & Strahilevitz, *supra* note 81 (showing a significant negative effect of age on privacy expectations against government surveillance in Table 4 such that older people had lower expectations); Matthew B. Kugler & Thomas Rousse, *The Privacy Hierarchy: Trade Secret and Fourth Amendment Expectations*, IOWA. L. REV. (forthcoming 2019) (showing a negative effect of age on privacy expectations in the law enforcement context, but no effect in the corporate surveillance domain).

of customer loyalty program as much as older people. Or perhaps younger people place greater value on automated check-in and ordering.[84]

B. Willingness to Pay

Participants also completed a willingness-to-pay style question in each domain. The nature of this question necessarily varied by context. In the case of the coffee shop loyalty program, the question described a customer loyalty program (administered using either cards or biometrics) and asked whether the survey respondent would want to participate. Were the program card-based, 77.0% would want to participate in exchange for every tenth coffee free. On average, only 46.6% would want to participate if the program used biometrics. Results from all conditions are reported in Table 2.

The gym and employment domains did not lend themselves to so natural a question. Likely an employer or gym would either have biometrics, or it wouldn't. The author is aware of no program by which an employer or gym has an "option" of using biometric check-in that it incentivizes with a reward. The willingness-to-pay questions here were therefore somewhat more artificial. Participants in the biometric conditions for these two domains were asked whether they would be willing to pay some amount of money to switch to a non-biometric check-in procedure. On average, 44.4% in the gym domain and 33.3% in the employment domain said they would be willing to pay some amount.[85] Though it may seem odd to have an employee pay an employer for a benefit like this, employers regularly take payroll deductions for employee parking and other optional employment benefits.

Within each domain, some interesting patterns emerged. For the employment domain, having a policy by which the information could not be shared and would be destroyed upon departure from the company made people less likely to be willing to pay.[86] Providing a justification did not have a significant effect.[87]

In the gym domain, providing those same kinds of assurances that the information would be contained had no significant effect.[88] There was, however, a

---

84. *See, e.g.*, Hayley Peterson, *Millennials' Hatred of 'Dealing with People' Is a Major Threat to Fast-Food Workings*, BUS. INSIDER (Aug. 29, 2016), https://www.businessinsider.com/millennials-hate-interacting-with-people-2016-8 [https://perma.cc/EUU3-VBYA].

85. In the gym domain, participants indicating a willingness to pay were asked how much they would be willing to pay assuming a baseline gym membership fee of $40 a month. The mean was $16.87 a month and did not vary significantly by condition.

86. A chi square was conducted using examining whether willingness to pay (yes/no) varied as a function of "destroy" (yes/no). This collapses across justification conditions. χ^2 (2, N = 249) = 6.33, p = .012

87. χ^2 (2, N = 249) = 1.58, p = .209. Given that providing a justification was non-significantly associated with greater comfort, one might wonder why it is also non-significantly associated with greater willingness to pay to opt out of the system. But consider that the justification was that biometrics limited an employee's ability to cheat the system. Though this might reassure the employees about the employer's intent, it does highlight the conflict in incentives.

88. χ^2 (2, N = 280) = .144, p = .705.

significant effect of the information being facial recognition data rather than thumbprint data such that more people were willing to pay to opt out of facial recognition use.[89]

Table 2: Willingness to Pay Questions by Domain

Coffee	**Percent Saying "Yes"**					
"Imagine this tracking of customers was used to administer a customer loyalty program that gave participating customers their every 10th coffee free. Would you participate in the program?"	Keycard 77.0%	Average Biometric 46.6%	Thumb Retain 43.3%	Thumb Destroy 44.4%	Face Retain 40.0%	Face Destroy 58.6%
Gym						
"Imagine you had the option of paying more and checking in with a card or keychain tag instead of using this other method. Would you be willing to pay some amount of money more per month?"		Average Biometric 44.3%	Thumb Retain 44.3%	Thumb Destroy 30.9%	Face Retain 42.0%	Face Destroy 62.3%
Employer						
"Would you pay some amount of money for your company to use a card or keychain tag to check in instead of your thumbprint information?"		Average Biometric 33.3%	Thumb Retain Justified 43.8%	Thumb Retain Not Justified 36.1%	Thumb Destroy Justified 28.3%	Thumb Destroy Not Justified 21.8%

Note: In the coffee domain, a "Yes" answer indicates a willingness to participate in a program despite data collection. In the other two domains, a "Yes" answer indicates a willingness to pay to opt out of such a program. Since the gym and employer cases involved willingness to pay to switch to a keycard regime, the question was not asked in the control conditions.

In the coffee shop domain, interest in participating in the loyalty program did not significantly vary based on either type of biometric data or data retention policy.[90] Since the coffee question merely asked whether the participant wanted to

89. χ^2 (2, N = 280) = 6.86, p = .009.
90. χ^2 (2, N = 270) = .801, p = .371 and χ^2 (2, N = 270) = 2.86, p = .091, respectively.

be in the loyalty program, however, it was possible to compare the responses in the control condition to those in the four biometric conditions overall. People were significantly less likely to want to participate if the program worked via biometrics, with 77% wanting to participate in the control condition and only 46.6% wanting to participate in the biometric conditions.[91]

In all three domains, then, a meaningful number of people either expressed a willingness to give up a benefit in exchange for avoiding a program that used biometrics (coffee shop) or a willingness to pay to opt out of a biometric program (gym and employer). These participants appear to have translated their increased discomfort with biometric programs into avoidance of them. The nature of the biometric program, whether it was facial recognition or thumbprint based and whether it had a privacy-attentive data retention policy, had inconsistent effects. But the general concern with biometrics programs was reliable across contexts.

III. WHY PROTECT BIOMETRIC PRIVACY

The previous Section shows that many people do value biometric privacy and that they are willing to sacrifice benefits in order to preserve it. This raises the question discussed at the beginning of the paper: why? What is the point of biometric privacy?

A. BIPA's Motivations and Other Possible Rationales

Since BIPA is by far the most expansive of the laws currently protecting biometric privacy, it is instructive to consider why it was passed and what its advocates considered its primary purpose. The specific motivating event for the passage of BIPA was the bankruptcy of a firm called Pay by Touch.[92] This company's principal product was a payment system that allowed people to complete a retail transaction with a fingerprint.[93] When the company filed for bankruptcy in 2007, one of its primary assets was its trove of consumer fingerprint and financial records.[94] The privacy ombudsman in the case excluded the biometric data from sale because selling or licensing the data would have violated Pay by Touch's privacy policy: "Pay By Touch will not rent, sell, license, or lend your [personally identifiable information] to third parties for advertising or marketing without your consent."[95] Nevertheless, Pay by Touch's records had contained data from a large number of Illinois residents. The prospect that this compilation of information could have been sold was enough to spur the Illinois legislature into action.

---

91. χ^2 (2, N = 405) = 33.83, $p < .001$.

92. The story of this case is reviewed in Lucy L. Thomson, *Sensitive Personal Data for Sale in Bankruptcy—An Uncertain Future for Privacy Protection*, 2017 ANN. SURV. BANKR. L. 12 (2017); *see also* H.R. Deb., 95th Gen. Assemb., at 249 (Ill. 2008) (statement of Kathy Ryg), available at http://www.ilga.gov/house/transcripts/htrans95/09500276.pdf [https://perma.cc/Z6J2-42A3].

93. Thomson, *supra* note 92.

94. *Id.*

95. *See id.*; 11 U.S.C.A. § 332.

The legislative debate surrounding BIPA is notable for the absence of those actors who have subsequently expressed the greatest opposition. None of the witnesses who appeared, testified, or submitted written statements regarding BIPA were affiliated with the technology industry. Only one witness—James Ferg Cadima of the American Civil Liberties Union (ACLU)—spoke on the record in any surviving committee discussion.[96] Most of the witnesses who submitted witness slips—but do not appear to have spoken on the record—represented interests related to state or local government.[97] Though two witnesses marked that they were opposed in the early stages of the committee discussion—one each from Cook County and the state police—subsequent amendments exempting government agencies and government contractors appear to have alleviated their concerns.[98] There is no evidence of any lobbying, or even awareness, by Silicon Valley. This is, unsurprisingly, no longer the case. Biometric legislation is now fiercely contested by Facebook and Google, among others.[99]

The text of the bill and the legislative history presents data security as the primary justification for treating biometrics as special. According to the statute,

96. Transcript of House Rules Committee meeting on May 28, 2008 (on file with author). The Senate Committees do not record their sessions and no witness spoke on the floor of either body.

97. Bill Folder of Senate Bill 2400, 95th Illinois Gen. Assemb. (on file with author). Of the eleven unique witnesses to have submitted witness slips for either chamber's committee meeting, two were from the Illinois Secretary of State's office, two represented law enforcement, one each came from the Chicago of Chicago and Cook County, and one represented the American Federation of State, County, and Municipal employees. The remaining witnesses were James Ferg Cadmina from the ACLU and three representatives of banking or medical interest groups.

98. *See* S.B. 36 (Ill. 2018), S. Comm, Amendment 1 (exempting public agencies involved in criminal investigations or issuing driver's licenses, which is a major task of the IL Secretary of State's office); H. Comm. Amendment 1 (fully exempting public agencies and also financial institutions subject to the Gramm-Leach-Bliley Act of 1999). Two representatives of a banking lobby group were also present at the committee meetings, and H. Comm. Amendment 1 also exempted much of their industry. An interview with James Ferg Cadima (July, 9, 2018) and subsequent correspondence confirms what is apparent from the record: the only major opposition to the bill was from government actors that were concerned they would be unable to ensure their own compliance, and this opposition evaporated after the amendments were added. The medical lobbyists were similarly neutral after the amendment passed.

99. *See, e.g.*, Russell Brandon, *Facebook-backed Lawmakers Are Pushing to Gut Privacy Law*, VERGE (Apr. 10, 2018), https://www.theverge.com/2018/4/10/17218756/facebook-biometric-privacy-lobbying-bipa-illinois [https://perma.cc/5DRP-4JD7] (discussing attempts by Illinois legislators to revise BIPA's provisions); April Glaser, *Facebook Is Using an "NRA Approach" to Defend Its Creepy Facial Recognition Programs*, SLATE: FUTURE TENSE (Aug. 4, 2017), http://www.slate.com/blogs/future_tense/2017/08/04/facebook_is_fighting_biometric_facial_recognition_privacy_laws.html [https://perma.cc/KZ9U-TZ6E] (discussing Facebook's attempts to kill BIPA); Kartikay Mehrotra, *After Facebook Lobbying Failed, Google Takes Aim at U.S. Law Banning Use of Biometric Data Without Consent*, JAPAN TIMES (Apr. 26, 2018), https://www.japantimes.co.jp/news/2018/04/26/world/facebook-lobbying-failed-google-takes-aim-u-s-law-banning-use-biometric-data-without-consent/#.XXLZF5NKjdd [https://perma.cc/2VBY-HWKT] (discussing Google's attempt to propose BIPA revisions); Sara Merken, *New Illinois Attorney General Ready for Biometric Privacy Fight (1)*, BLOOMBERG L. BIG L. BUS. (Nov. 8, 2018), https://biglawbusiness.com/new-illinois-attorney-general-ready-for-biometric-privacy-fight-1 [https://perma.cc/A67L-GV3P] (discussing the role of the new Illinois Attorney General in the ongoing legislative debates).

BIPA was enacted because biometric information is "biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[100] The whitepaper submitted by the ACLU in support of the bill—the only written submission in the legislative record—and comments on the floor in support of the bill affirm this data security purpose.[101]

Biometric information, whether a thumbprint, a voiceprint, or a record of facial geometry, can be seen as the worst form of password. It is both common to multiple vendors—you have only one thumb on each hand—and unchangeable. It is even, as discussed above, semipublic. This leads to the fear that a data breach or sale by one holder of a piece of a person's biometric information would compromise the security of all relationships that are verified by that same piece. And, once compromised, the very nature of biometrics would make it impossible to regain security; biometrics are hard to alter. This is why the immutability of biometrics and concerns about identity theft appear so often in discussions of biometrics. As one scholar put it, "Essentially, biometrics are the equivalent of a PIN that is impossible to change. The theft of biometric information amounts to permanent identity theft, and thus may be extremely difficult to counteract."[102]

There is an entire literature now on the security of biometric systems, with teams of researchers regularly seeking to beat current biometric security and to design around known weaknesses.[103] Notably, however, most of these studies do not begin with the assumption that biometric information has been stolen from one database and then is being used to hack another—the model that seemed to concern the sponsors of BIPA. Instead, these researchers often presume access to some trove of information, such as a user's pictures on social media or a latent fingerprint,

---

100. 740 ILL. COMP. STAT. 14/5(c).

101. AMERICAN CIVIL LIBERTIES UNION, GETTING AHEAD: THE NEED TO ESTABLISH BASIC BIOMETRIC PROTECTIONS IN ILLINOIS (Submitted in support of S.B. 2400 May 28, 2008) (on file with author) ("The unique nature of biometrics . . . leaves a growing number of Illinoisans at heightened risk of financial loss/identity theft."); *see also* Transcript of the State of Illinois 95th General Assembly House of Representatives 249 (May 30, 2008) (on file with author).

102. Steven C. Bennett, *Privacy Implications of Biometrics*, PRAC. LAW. 13, 16–17 (2007).

103. *See, e.g.*, Kai Cao & Anil K. Jain, *Hacking Mobile Phones Using 2D Printed Fingerprints*, MSU TECHNICAL REPORT (Feb. 19, 2016), http://biometrics.cse.msu.edu/Publications/Fingerprint/CaoJain_HackingMobilePhonesUsing2DPrintedFingerprint_MSU-CSE-16-2.pdf [https://perma.cc/J26B-LJWA] (using printed images of fingerprints to access iPhones); Judith Myerson, *How to Fool a Fingerprint Sensor*, ELECTRONIC PRODUCTS (Mar. 13, 2017), https://www.electronicproducts.com/Mobile/Devices/How_to_fool_a_fingerprint_sensor.aspx [https://perma.cc/TZ4R-X7T9] (discussing the strengths and weaknesses of different types of fingerprint scanners and their relative susceptibility to hackers); Corey Nachreiner, *Passwords: 4 Biometric Tokens and How They Can Be Beaten*, DARKREADING (Jan. 31, 2018), https://www.darkreading.com/operations/passwords-4-biometric-tokens-and-how-they-can-be-beaten/a/d-id/1330939 [https://perma.cc/P5U5-UC22] (reviewing a variety of biometric security possibilities and assessing their weaknesses); Lily Hay Newman, *Hackers Trick Facial-Recognition Logins with Photos from Facebook (What Else?)*, WIRED (Aug. 19, 2016), https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/ [https://perma.cc/M5MX-V22X] (describing a project that tricked facial recognition technology using images of a user's face taken from social media).

and then see whether enough information can be extracted from this source to beat a scanner. It is unclear whether BIPA meaningfully protects against this sort of attack. In one proof-of-concept study that is somewhat closer to the BIPA model, however, researchers were able to beat an iris scanner by reconstructing what the original iris must have looked like based on the stored data captured by a biometric scanner.[104]

Though the legislative findings recorded in the text of the statute lead with concern over identity theft, there is also some mention of other issues. Specifically, the legislature pointed to popular fear over use of biometrics and the uncertainties inherent in this new technology.[105] In the ten years since the statute was passed, the discussion of biometrics has shifted more to concerns over how biometrics can enable public tracking, specifically a fear that increased use of biometrics to monitor public spaces could lead to the death of anonymity. This rationale is in part what motivated Microsoft to call for greater regulation of facial recognition,[106] and it was also stressed in an ACLU amicus brief filed with the Illinois Supreme Court in the recent *Rosenbach* case.[107] Certain kinds of biometric data allow for the possibility of public tracking via security cameras, and the possibilities for future growth in this area are immense.[108] A single image of a face at a public event could rapidly be identified by consulting one database and then linked to an endless stream of

104. Kim Zetter, *Reverse-Engineered Irises Look So Real, They Fool Eye-Scanners*, WIRED (July 25, 2012), https://www.wired.com/2012/07/reverse-engineering-iris-scans/ [https://perma.cc/94D3-4DQN].

105. 740 ILL. COMP. STAT. 14/5(d–f).

106. *See* Harwell, *supra* note 2.

107. Brief of Amici Curiae the American Civil Liberties Union, The American Civil Liberties Union of Illinois, the Center for Democracy & Technology, the Chicago Alliance Against Sexual Exploitation, the Electronic Frontier Foundation, Illinois PIRG Education Fund, Inc., and Lucy Parsons Labs in Support of Plaintiff-Appellant at 3, Rosenbach v. Six Flags Entm't Corp., No. 123196 (Ill. July 6, 2018), available at http://www.illinoiscourts.gov/SupremeCourt/SpecialMatters/2016/123186_AMB.pdf [https://perma.cc/TE43-S8JG] ("Without reasonable limits, biometric technologies threaten to enable corporations and law enforcement to pervasively track people's movements and activities in public and private spaces, and risk exposing people to forms of identity theft that are particularly hard to remedy."). This case has now been decided. See *supra* note 17 and accompanying text.

108. *See* Bennett, *supra* note 102, at 17 (speculating that this could lead to the end of anonymity and the suppression of dissent); Blitz, *supra* note 46, at 1410–11 (discussing how public tracking via video surveillance would curtail First Amendment freedoms); Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113, 1126 (2015) ("Extensive surveillance can produce both conformity and anxiety. When the government wields public surveillance as a tool, this shifts the balance of power between citizens and government, and makes citizens less able to effect democratic change."); Sharon Nakar & Dov Greenbaum, *Now You See Me, Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. SCI. & TECH. L. 88, 99 (2017) ("Soon, if not already, simply by walking past a store putative customers might be identified by camera, and be alerted about sales in the vicinity . . . . There are already billboards that engage with passing costumers by using simplistic facial-recognition software that can identify the costumer gender, age, and even their mood . . . . Stores and casinos also use this technology to prevent previously identified unwanted guests like card counters and shoplifters from entering.").

personal information as that database is connected to others.[109] This presents a substantial problem if one values the idea of public anonymity. And here the immutable nature of biometrics is indeed troubling; once your facial geometry is out there, it can be used to track you until your appearance drastically changes. In general, this public tracking concern is more applicable to facial geometry and perhaps voiceprints than to fingerprints, but it is difficult to predict where future technological advances may take us. For example, long range iris scans are now technologically feasible, meaning that many of the arguments about facial recognition tracking in public apply there as well.[110]

A broader framing of this concern focuses on uncertainty about what biometrics might enable in the future. Biometric technology is fairly new, and new technologies can fundamentally change our understandings of privacy even in very short periods. The first iPhone was released in 2007. Only seven years later the Supreme Court held that smartphones are special for privacy purposes—they had become so integrated into our daily lives that to pretend they were simply oddly-sized briefcases would have been absurd.[111] And in 2018 the smartphone-driven legal revolution continued, with long-held assumptions about privacy interests in third-party held location data being overturned in the cell phone context.[112] Right now, biometrics data is being collected by a host of apps and smart-home style devices.[113] This type of data is generally not well-protected by current privacy law.[114] The downstream implications of this are, at best, unclear.

A final set of concerns involves the uniquely personal nature of biometrics. A person's face is part of them in a way that their social security number or identity card is not—no government or corporation issued them their biometrics. This is an argument that sounds in dignity more than practicality, but we should not be too quick to reject the notion that biometrics are more revealing than is immediately

---

109. Bennett, *supra* note 102, at 17.

110. Robinson Meyer, *Long-Range Iris Scanning Is Here*, ATLANTIC (May 13, 2015), https://www.theatlantic.com/technology/archive/2015/05/long-range-iris-scanning-ishere/393065/ [https://perma.cc/JNK8-QPYK] (quoting the creator as saying, "Unlike other scanners, which required someone to step up to a machine, his scanner can capture someone's iris and face as they walk by."); *see also* Kien Nguyen et al., *Long Range Iris Recognition: A Survey*, 72 PATTERN RECOGNITION 123, 139 (2017), available at https://www.cse.msu.edu/~rossarun/pubs/NguyenLongRange Iris_PR2017.pdf [https://perma.cc/5E7D-HY4B].

111. Riley v. California, 134 S. Ct. 2473, 2488 (2014) ("That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.").

112. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

113. Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 452 (2018).

114. *See, e.g.*, Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 95 (2014) ("Both state and federal consumer protection law has not yet addressed these problems or the general issues that the Internet of Things creates for consumer consent.").

apparent. Recent research has suggested that it is possible to predict sexual orientation from facial geometry, for example.[115]

Though discussions of BIPA's purpose largely focused on data security rather than these other concerns, we should not assume the sponsors of BIPA were unaware of the possibility that future developments would raise other privacy issues. BIPA was very broadly written, and its strong focus on notice and consent serves an information-forcing function. Under BIPA, companies must give notice when they collect biometrics and of what they intend to do with them.[116] Absent such legislative protection, the public would likely have a very poor idea of when and to what end biometric information is being used. BIPA forces biometric use out into the public, where it can be debated. BIPA also stated that its purpose was to make people feel safer when engaging in biometrically facilitated transactions by alleviating some of their privacy concerns, which arguably makes preventing consumer discomfort one of its central goals.[117]

B. Empirical Data on Explanations and Justifications

Immediately following the biometric scenarios presented in Part II, participants answered questions assessing their general level of comfort with biometric information collection by commercial entities. The questions were prefaced by a brief explanation of how biometric information could be used. Participants were told that a store might ask a customer to scan a fingerprint rather than swipe a card to access a customer rewards account or use facial recognition to suggest favorite orders. The full text of these prompts is included in the Appendix.

Participants were then given separate explanations of fingerprint and facial recognition biometric procedures and asked to rate their level of comfort with a company having each if that company had the right to use the information however it wished. Comfort ratings were given on scales ranging from 1-6, with higher numbers indicating greater comfort.[118]

---

115. *See* Derek Hawkins, *Researchers Use Facial Recognition Tools to Predict Sexual Orientation. LGBT Groups Aren't Happy,* WASH. POST (Sept. 12, 2017), https://www.washingtonpost.com/news/morning-mix/wp/2017/09/12/researchers-use-facial-recognition-tools-to-predict-sexuality-lgbt-groups-arent-happy/?noredirect=on&utm_term=.adb67e4e5ff7 [https://perma.cc/VFQ5-8UGJ]; Yilun Wang & Michal Kosinski, *Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation*, OSF HOME (Feb. 15, 2017), https://osf.io/zn79k/ [https://perma.cc/FBU3-PUNA].

116. 740 ILL. COMP. STAT. 14/15.

117. 740 ILL. COMP. STAT. 14/5.

118. Participants who had seen the coffee shop vignette in the first part of the study reported that they were less comfortable with biometric data collection here. Since the coffee shop vignette is closest to this policy application, it seems that greater detail about this kind of program leads to even less comfort with it. The explanations selected by comfortable and uncomfortable participants did not vary as a function of prior biometric vignette, however. Tables available from the author.
Here are the results for the two comfort measures. Fingerprint: $F(2, 1223) = 5.59$, $p = .004$, $\eta^2 = .009$. Coffee (M = 2.12, SD = 1.57); Gym (M = 2.45, SD = 1.73); Employer (M = 2.48, SD = 1.74). Facial Recognition: $F(2, 1223) = 5.65$, $p = .004$, $\eta^2 = .009$. Coffee (M = 2.17, SD = 1.56); Gym (M = 2.53, SD

Because the scale had an even number of points, and therefore no midpoint, it was possible to split respondents into those who reported being at least somewhat comfortable or at least somewhat uncomfortable with biometric collection. For both facial geometry information and fingerprint information, 74.6% of participants reported being at least somewhat uncomfortable. A pilot for this study conducted on Prime Panels—another provider that was tasked with providing a less representative set of respondents—found 73.4% discomfort for fingerprint information and 76.8% discomfort for facial geometry information, so this fairly extreme result has replicated.

Each participant then received separate follow-up questions for fingerprint and facial geometry biometric information asking them why they were or were not comfortable, whichever was appropriate given their previous responses. Participants were able to select multiple reasons from a list and could also provide their own alternative explanation for their feelings. The list of potential reasons was generated from a review of the arguments made in discussions of biometric privacy and was supplemented by suggestions from research assistants. There were no large differences in the reasons selected for fingerprint and facial recognition information, but percentages are listed separately for greater clarity.

= 1.73); Employer (M = 2.47, SD = 1.68). Differences between coffee shop and the other vignettes are significant at the $p < .05$ level.

Table 3: Reasons for Comfort or Discomfort with Biometric Information Collection.

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%

Note: Text in the survey substituted "facial geometry" and "fingerprint" as needed. The "Other" option always appeared last, but the other choices appeared in random order.

A review of the reasons for discomfort suggests that concern about biometric data collection comes from many sources.[119] Four different rationales were selected by at least half of the sample. The most commonly chosen rationale was that it felt very invasive for a company to collect and share the information (70% overall). Perhaps unsurprisingly, given the prior discussion of facial recognition databases and the proliferation of cameras in public places, 67% said that they were worried where the collection of biometric information might lead in the future. Similarly, 63% selected an option that specifically mentioned tracking in public when considering facial geometry information, though only 55% mentioned it for fingerprints. Finally, 55% said they were concerned that collection of this information could lead to identity theft. Interestingly, only a small minority cited two reasons that are frequently mentioned in the literature: that biometrics cannot be changed, and that biometric information is "part of me."[120]

119. *See* Table 3.
120. *See e.g.*, *supra* note 102 and accompanying text.

Only one reason for *comfort* attracted near majority support. For fingerprint data, 57% said that they had nothing to hide that fingerprint information would reveal. For facial geometry information, 50% said likewise. All other explanations attracted less than a third of the sample each. In a somewhat surprising turn, only 28% said that facial geometry information was already public.

These results are strongly supportive of a multi-factor approach to biometric privacy harms. Though participants are concerned about data security and identity theft—perhaps correctly, perhaps not—they are also, and in fact more, concerned about several other factors. And it is hard to dismiss these other concerns as products of ignorance because facial recognition can be used to track people in public, long range iris scanners in the tradition of Minority Report are technologically feasible, and we don't know what other uses will become possible in the years ahead.[121]

IV. WHAT USES MAKE PEOPLE UNCOMFORTABLE?

The previous data shows that at least some uses of biometric technology concern people, and that a meaningful number of people are willing to incur costs to avoid having their biometric information collected and used. Biometric technology can be used in many different ways, however, and some of those ways seem less intuitively troubling than others. One can unlock the latest model iPhones using facial recognition, and the biometric data that enables this is stored only on your own device.[122] For many, this might feel less intrusive than a store using facial recognition to track your shopping patterns even if both are uses of the same technology.

When thinking about biometric technology policy, it is important to consider a wide range of possible uses. Should the law distinguish between a bank using your voiceprint to confirm your identity from a department store using your facial geometry to serve targeted advertisements? Is it a problem if a store initially collects biometric data for one purpose and then decides to use it for another without obtaining fresh consumer consent?

To help answer these questions, a second study was conducted. This study drew its panel from Dynata, the successor company to Research Now/SSI. Again, the demographics of the sample were set to match U.S. census proportions on the dimensions of age, sex, region, education, and race/ethnicity. Full demographics are reported in the Appendix. The final sample contained 1029 individuals.[123]

---

121. *See supra* notes 3–4, 104, and accompanying text.

122. The Associated Press, *How Does Apple's Face ID Work and Will It Store My Face in the Cloud?*, HAMILTON SPECTATOR (Sept. 27, 2017), https://www.thespec.com/news-story/7580403-how-does-apple-s-face-id-work-and-will-it-store-my-face-in-the-cloud-/ [https://perma.cc/BEA5-R3RA].

123. As with the first study, inattentive participants were screened from the final sample based on two criteria. First, participants who did not give the appropriate response to either of two attention check questions—questions asking participants to give a particular response—were unable to complete

In the first study, the point had been to assess how people felt about biometric technologies when they were presented as part of a relatively rich vignette. Here, the purpose was to examine how people felt about different uses of biometrics compared to one another. Rather than presenting participants with lengthy stories, therefore, this study gave brief, one-sentence descriptions of business uses of biometrics. Participants were asked to rate how comfortable they were with these uses on scales ranging from 1 – Very Uncomfortable to 6 – Very Comfortable. The full text of the questions is given in the Appendix. The items were administered in quasi-random order.[124]

As can be seen in Table 4, people were much more comfortable with some uses of biometric technology than others. In general, people seemed most comfortable when biometrics were being used for security purposes or in place of passwords. For instance, people were fairly comfortable with using either fingerprint (71.1% comfortable) or facial recognition (58.9%) biometrics to unlock a phone. They were also more comfortable than not with using biometrics to unlock an app (65.0% comfortable) or verify an identity when calling a credit card company (54.9%).

People were much less comfortable, however, with the next generation of biometric uses. Using facial recognition to track people on public streets (68.1% *uncomfortable*), detect photos of celebrities online (73.8%), or to link profiles of people across social networking sites (69.1%) made majorities uncomfortable.

Driving home this distinction, 58.9% of people were comfortable with a store using facial recognition to detect when people who were banned from the store, such as previously apprehended shoplifters, had entered. But only 25.8% were comfortable with the store using facial recognition to track customer interest for serving advertisements.[125] The same actor, using the same technology, was evaluated quite differently depending on the goal of the use.

---

the study. Second, participants were screened from the final sample if they finished the study in less than one-third of the time taken by the median participant.

124. To reduce subject fatigue, the eighteen items were splits over three pages with six items to a page. A programming limitation prevented fully randomizing item presentation across these pages, however. Instead items were randomly assigned to one of three blocks (each being a page) and then both the order of block presentation and the order of questions within each block was separately randomized for each participant. Since doing this block randomization only once would have led to Item A always being in the same block as Item B—potentially giving rise to neighbor effects—three separate sets of block assignments were created. The end result is not perfectly random but is close. There were no significant differences in comfort ratings across block assignments (no $p < .05$ after correction for multiple comparisons).

125. The wordings of these two items are below:

A department store like Walmart or Home Depot using facial recognition to detect when people who have been banned from their stores—for example, people caught shoplifting—have entered.

A department store like Walmart or Home Depot uses facial recognition to track where individual customers go in their stores and what items those customers look at, so they can later send those customers targeted advertisements.

Table 4: Comfort with Different Uses of Biometric Technology.

	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: Means with standard deviations in parentheses.

Currently, biometrics laws do not sort between these kinds of uses. BIPA, for instance, has exemptions for banks and financial institutions,[126] but it does not distinguish between a store using facial recognition to exclude known bad actors from one using biometrics to facilitate marketing. Second generation biometrics laws should begin to discriminate between these kinds of cases. According to these data, there is a world of difference between an employer taking a fingerprint for check-in and a homeowner's association or technology company instituting public tracking via facial recognition. Perhaps it is reasonable to say that the employer need not get explicit consent for fingerprint check-in whereas the homeowner's

126. 740 ILL. COMP. STAT. 14/25(c).

association must for public tracking. Perhaps stores should operate under different restrictions depending on whether they use biometrics solely for security. Thus far, however, these distinctions do not matter doctrinally.

These data also support the point made in Part III about fear of public tracking. The most discomforting uses of biometric technology all involve the use of facial recognition to follow people in public spaces. And, as the store questions make clear, people are deeply sensitive to the purpose of a tracking regime. This suggests that we should be very concerned about "purpose creep" in the biometric context.

These data also support a notice-based regime. People care why data is being collected and how it is being used. For people to appropriately judge how they feel about an actor's use of biometrics, however, they must know about it. If someone wants to boycott a store or bank because it uses biometric security, or specifically choose one because it does, then that is democracy at work. But people cannot have informed choice without notice.[127]

V. IMPLICATIONS

A. For the Value of Biometric Privacy

Taken as a whole, these data show that many people value biometric privacy and that they take a broad view of possible biometric privacy harms. In each domain in the first study, people were significantly less comfortable with a check-in or tracking regime if the regime worked via biometrics rather than ID cards. This is a non-obvious result. One could defensibly argue that the main privacy or dignity violation is the tracking regime itself, that people don't want to have to punch a time clock or have their every check-in at the gym or coffee shop permanently recorded. But these data show that there is an additional cost to comfort when these records are created via biometrics and biometric information is saved alongside the other data.

One might express concern that participants are overly focused on the biometric elements of these scenarios. But the scenarios attempted to present the check-in and customer loyalty procedures in as straightforward and matter-of-fact a manner as possible. The main comfort questions do not even mention biometrics, simply referring to the check-in and data retention policies overall. The willingness-to-pay questions, which did reference biometrics explicitly, appeared on a separate page, and the biometric policy questions that laid out biometric issues in more detail came after those on their own page.

---

127. Kaminski, *supra* note 108, at 1136. ("Requiring notice allows the surveillance subject to recalculate her mechanisms for maintaining an optimized balance of openness and closedness in a given environment . . . . Notice can also trigger social enforcement through shaming of the person conducting surveillance.").

Further, many participants report that they would be willing to pay to switch from a biometric regime to a non-biometric regime. Approximately a third of the participants in the employment case and over 40% in the gym case would be willing to pay some amount of money to switch from biometrics to ID cards. These data could be criticized as cheap talk because participants are neither being asked to spend their own money nor being presented with the kind of choice they regularly encounter. But the coffee shop loyalty program is much more naturalistic. Participants were told that the coffee shop's loyalty program worked in a certain way and that, if they participated, they would get every tenth coffee free. If the program happened to work via ID cards, 77% wanted to participate. If it happened to work via biometrics, only 47% wanted to participate. For such a minor change, this was a substantial difference in uptake and was observed when considering the kind of choice that people might realistically face in their daily life.

Providing assurances that data would only be kept for as long as it was needed and would not be used for other purposes meaningfully increased comfort in the employment case, and led to fewer people expressing willingness to pay to opt out there. This suggests that the BIPA requirements—which the "destroy" conditions were intended to mirror—actually do provide some reassurance to employees and consumers. And, since many current BIPA cases are employment related, these data may be particularly relevant to ongoing litigation.

But the effect of these use and security limitations was less clear in the coffee and gym conditions, with the effect on comfort being weaker (and occasionally non-significant) and the willingness-to-pay data being mixed. Likely, the social understandings of employment relationships differ from those of consumer relationships, and these different background assumptions play a role in these divergent effects. One possibility is that employees are already accustomed, by necessity, to trusting their employers not to misuse other kinds of sensitive information. Employers already know social security numbers, salary amounts, health insurance choices, and family status, for example. So, while employees may be primed in the employment context to extend further trust when biometric information requirements are coupled with confidentiality assurances, there is no similar model for gyms or coffee shops. The modal barista is likely trusted with your order preferences, the frequency of your visits, and whether you tip or are nice to them. Though these pieces of information are arguably also revealing, they are not of the same caliber.

B. For Theories of Biometric Harm

Returning to theories of biometric harm, these data show that people are taking a broad perspective. No single theory of harm dominates for people concerned with biometric data collection, and many participants are attributing their discomfort to multiple sources. Many say that biometric data collection and sharing feels invasive (dignity). But many also express concerns about public tracking and the future harms that may be enabled by biometric data usage (tracking in public)

and identity theft (security). This suggests that the data security focus that dominated early discussions of biometric privacy misses a meaningful portion of what now concerns people. Courts wanting to take biometric privacy seriously would do well to consider the multifaceted nature of biometric privacy concern and not shortchange either the dignity features of biometric privacy or the downstream consequences of biometric data collection.

Further, the second study shows that not all uses of biometrics are the same. Some uses were concerning only to a small minority, but some made a strong majority uncomfortable. This simple insight suggests that the current litigation over Illinois's biometric privacy statute has led some people astray. Courts are trying to decide whether it causes you harm when a company collects your biometric information *if they do not disclose it*.[128] These data suggest that this is exactly the wrong question. Courts should instead be asking whether it causes you harm when a company collects your biometric information given *what they do with it*. Some uses may cause harm, and others may not.

As we craft new biometric privacy laws, we should not argue about how sensitive this or that piece of biometric information is—that leads into the trap of asking whether your face is private. Instead, we should ask what kinds of activities we want to enable. It appears, based on these data, that there would be a majority in favor of using biometrics to make banking more secure. There is also a strong majority in favor of not using biometrics to track people in public for the purpose of marketing. There is much more work that can be done to flesh out these results—among other things, one can ask whether "majority" is the appropriate standard—but these data set a few guideposts that may serve to begin the discussion.

C. For Standing Doctrine

These results can inform the question of standing in federal courts. Numerous federal courts have been confronted with the question of when a violation of the notice and consent provisions of a biometric privacy statute gives rise to Article III standing.[129] 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."[130] 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 recent *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

128. *See, e.g.*, McGinnis v. United States Cold Storage, Inc., No. 17 C 08054, 2019 WL 95154, at *4 (N.D. Ill. Jan. 3, 2019); *see also supra* note 20.

129. *See supra* note 20 and accompanying text.

130. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).

'actual or imminent, not conjectural or hypothetical.'"[131] 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.[132]

In the context of this sort of privacy class action, particularization is not a major problem. A particular person's biometric data is allegedly being 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*[133] and *Friends of the Earth, Inc. v. Laidlaw Environmental Services*,[134] both concerned environmental regulations. 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.[135]

Though particularity is not a major problem in the biometric privacy domain, concreteness is often a serious issue.[136] 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.[137] In his majority opinion in *Spokeo*, Justice Alito states 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.[138]

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."[139] 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."[140]

---

131. *Id.* at 1548 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).

132. *Id.* at 1550 (analysis of the circuit court below was "incomplete" because it "failed to fully appreciate the distinction between concreteness and particularization"). For further discussion of this point, *see, e.g.*, James E. Pfander, *Standing, Litigable Interests, and Article III's Case-or-Controversy Requirement*, 65 UCLA L. REV. 170, 213–17 (2018) (discussing the Court's concreteness and particularity requirements in *Spokeo*).

133. 504 U.S. at 565–68.

134. Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., 528 U.S. 167, 180–81 (2000).

135. *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).

136. 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.").

137. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013) (describing the standard for probabilistic harm).

138. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

139. *Id.*

140. Lujan v. Defs. of Wildlife, 504 U.S. 555, 580 (1992)

This semi-deference to legislative judgments about harm leads Justice Alito into a distinction between a "bare procedural violation" and actual harm.[141] 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.[142] 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.[143] If a plaintiff's credit report nonetheless remains accurate, however, they cannot establish concrete harm despite the consumer reporting agency's technical violation.[144] Further, in Alito's view, not even all inaccuracies in credit reports cause concrete harms.[145] An incorrect zip code in a credit report, for example, does not, "without more," "cause [concrete] harm or present any material risk of harm."[146]

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.[147] 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

---

141. *Spokeo*, 136 S. Ct. at 1550.

142. *Id.*

143. *Id.*

144. *Id.*

145. *Id.*

146. *Id.* Justice Thomas's concurrence tracks a parallel but somewhat different course. In his world, a violation of a regulation that is intended for public good, such as one requiring a corporation to post a contact number on its website, does not give rise to standing to sue. However, violation of a private right, such as the right to have a consumer reporting agency follow "reasonable procedures to ensure maximum possible accuracy," would create individual standing because it concerns the accuracy of particular reports and implicates a right that belongs to a particular individual. *Id.* at 1553–54 (Thomas, J., concurring).

Since BIPA creates an individual right not to have one's information collected absent certain formalities and safeguards, Thomas would likely have to find standing in many cases because rights created by BIPA are more "private" than "public."

147. S*ee, e.g.*, Kazim Ladimeji, *Should a Candidate's Commute Time Be a Selection Factor?*, RECRUITER (Mar. 4, 2014), https://www.recruiter.com/i/should-a-candidates-commute-time-be-a-selection-factor/ [https://perma.cc/BEA5-R3RA]; *see also* John Sullivan, *You Might Be Surprised How Much Commute Issues Hurt Hiring and Retention*, DR. JOHN SULLIVAN, https://drjohnsullivan.com/articles/you-might-be-surprised-how-much-commute-issues-hurt-hiring-and-retention/ [https://perma.cc/BU6S-KZGT] (last visited Sept. 5, 2019). Zip codes are also associated with the usual suite of neighborhood variables such as race and ethnicity, which are related to hiring preferences as well. *Id.*

in a variety of contexts.[148] It might be illegal to discriminate against someone because an error in their zip code led you to think they were the "wrong" race, but it may still happen.

If reasonable minds can be mistaken about the importance of something as simple as an errant zip code, something as complicated as biometric privacy seems destined to be a muddle. The question of whether some data collection or use practice is a substantive violation, a procedural violation, or a "bare" procedural violation simply returns us to the initial problem of defining what counts as a "concrete" harm.

To define "concrete" harm, let us consider concrete data. The results presented here show that people may have many different reasons for wanting to exercise control over how their biometric information is used. It is not enough that biometric data not be used to further identity theft; people are also concerned that this data is not mishandled in a variety of other ways. Many people would not, for instance, want to be tracked in public via their biometrics, and the mere collection of biometric information is enough to make some people meaningfully uncomfortable even without specific threats of downstream consequences. Recall the benefits that people were willing to give up, or costs that they were willing to accept, to not participate in biometric programs. If people say they would put money on the table to avoid a practice, then it seems odd to call that practice harmless. So, there is a wide range of potential substantive harms.

The procedural protections of BIPA also serve substantive purposes. This was the rationale recently adopted by the Ninth Circuit in finding standing in the Facebook photo-tagging case.[149] BIPA explicitly requires that the purpose of the data collection be disclosed and that the data subject agree to the collection in writing.[150] This insistence on informed consent fundamentally creates a bargain—"You can have my information if you do ____ with it and no more"—and the insistence on *written* consent creates a record of that bargain. One common problem in the privacy space is the discovery of new uses for old information.[151] Would people care if biometric information that was collected for one purpose was being used for another? The data in Part IV show that they would. A store would likely

148. *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].

149. Patel v. Facebook, Inc., No. 18-15982, 2019 WL 3727424, at *6 (9th Cir. Aug. 8, 2019) ("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.").

150. 740 ILL. COMP. STAT. 14/15 (2019).

151. *See, e.g.*, Ryan Dezember, *Your Smartphone's Location Data Is Worth Big Money to Wall Street*, WALL STREET J. (Nov. 2, 2018), https://www.wsj.com/articles/your-smartphones-location-data-is-worth-big-money-to-wall-street-1541131260 [https://perma.cc/Y3L7-TTQQ] (discussing how cellphone location information can be used to assess industrial productivity).

have the support of a majority of its customers if it wished to use facial recognition to better exclude those who had previously been banned from it. The store would likely be condemned by a supermajority of its customers, however, if it used the same information and same analytic techniques to track customers for advertising purposes. It is likely in recognition of such distinctions that the home improvement store Lowes used to reassure its customers that it *would not* use facial recognition to track customer preferences in this way and would *only* use it for security.[152] When there is a written contract it is much easier to establish what promises were made and implied in the moment of information collection.

The hardest case for standing is one in which a company collects biometric information in a manner that is completely open and uses the information only for a purpose that is completely obvious to those whose biometric data it has captured. Think, for example, of the employee timekeeping cases, where employees know why they are turning over their fingerprints, and of the *Take-Two* litigation, where video game players knowingly allowed a camera to capture their images so that the game could incorporate them into personalized avatars.[153]

One could argue the requirement of a writing serves a substantive purpose even in these cases. There are times when the law has recognized that apparently empty formalities serve a broader policy goal.[154] In the law of gifts, for example, it is important that the gifts are actually delivered to recipients in some form rather than merely promised, however earnestly.[155] The rationale behind this requirement is a concern with ensuring that the donor really means to give the gift.[156] This pickiness about procedural niceties is also the primary justification for the Statute of Frauds and its requirement that certain contracts be in writing rather than oral.[157]

A state would be in good company if it wishes to be similarly picky about the form in which consent is given. The European Union's (EU) General Data Protection Regulation, for instance, has explicit guidelines that attempt to avoid the problem of unread boilerplate consent,[158] and also requires that data collected for

152. LOWE'S, *supra* note 34 ("We do not use facial recognition or other biometric identifiers for marketing purposes or to build profiles of shoppers."). This policy is no longer in effect and has been replaced by one that does not offer the same guarantees. *See supra* note 34 and accompanying text. Lowes has declined the opportunity to comment on the change. Personal email from author, to Lowes.com Privacy Team (Aug. 14, 2018).

153. Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 15 (2d Cir. 2017).

154. *See, e.g.*, Felix Cohen, *Transcendental Nonsense and the Functional Approach*, 35 COLUM. L. REV. 809, 820–24 (1935).

155. Jane B. Baron, *Gifts, Bargains, and Form*, 64 IND. L.J. 155, 155–56 (1989) (explaining that the delivery requirement exists to ensure that donative intent has been correctly ascertained).

156. *Id.*

157. U.C.C. Law § 2-201 (AM. LAW INST. & UNIF. LAW COMM'N 1977) (contracts for sale of certain goods are unenforceable "unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought"); *see also* Carolyn M. Edwards, *The Statute of Frauds of the Uniform Commercial Code and the Doctrine of Estoppel*, 62 MARQ. L. REV. 205, 207 (1978) (noting that the historical purpose of the Statute of Frauds was "to provide reliable evidence of the existence of a contract" and prevent fraudulent claims).

158. General Data Protection Regulation 2016/679, 2016 O.J. L199, art. 7.

one purpose not be retained and used for radically different purposes.[159] It is hard to imagine that the EU would view "performative" consent as sufficient if a statute specifically called for written consent.

This insistence on written consent also creates a series of important incentives for corporate actors. When your employer collects your fingerprints to increase the accuracy of its timekeeping, it likely has no intention of using the data for other purposes. It may not, however, have devoted any attention to data retention schedules, data use restrictions, and data sharing possibilities. If your employer is required to comply with the formalities of BIPA, then it will be forced to take all these topics seriously and evidence its seriousness by posting a public privacy policy. This substantially increases the real level of protection that you will enjoy. If your employer can avoid these procedural requirements until it commits a more substantive violation, however, then it will likely be meaningfully sloppier in its data handling practices.[160] Importantly, merely not having a publicly posted policy would make it difficult for employees like yourself to detect just how sloppy it is being. We must therefore consider these forgone prophylactic benefits before declaring BIPA's technicalities "bare" procedure. The Illinois Supreme Court itself took exactly this view, saying that failure of a company to adhere to BIPA's "statutory procedures" makes an individual's biometric privacy rights vanish "into thin air," manifesting the "precise harm" the legislature sought to avoid.[161]

If courts are not willing to stretch federal jurisdiction quite so far, they still need to find standing in a wide range of other cases. Recall the multiple reasons why people might be concerned about the collection and retention of their biometric data. Even if the collection does not raise a data security concern, it could raise a public tracking concern. Even if it does not raise a public tracking concern, it may be a dignity violation. Only the truly open collection and truly limited use of biometric data requires one to argue that the harm comes from the lack of a writing itself.

The list of potential substantive violations is extensive. If people are unaware that their information is being collected, data collection violates their substantive right to *not* have their information collected without their consent. If their information is retained for longer than the law permits, is held in an unsecure manner, or is transferred to third parties without consent or for profit, substantive guarantees are also violated. If the information is being used in ways that are not readily apparent to users or that change after the information has been collected, that bait-and-switch too should count as a substantive violation.

The current round of biometric privacy litigation has gone after low-hanging fruit. It is easy to write a complaint saying that Company A violated the procedural

159. *Id.* at art. 5(1)(b).

160. Based on anecdotal comments, it appears that one of the challenges of bringing a company into compliance with BIPA is figuring out how the company has been storing biometric information. Often this was not previously considered an important question.

161. *See* Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186 ¶ 34 (Jan. 25, 2019).

requirements of biometric information collection. Often all plaintiffs' counsel needs do is: 1) know that the biometric is being collected, and 2) confirm that the data subjects were not given a privacy policy. If there is no standing to pursue these claims, however, then companies will not be forced the make the disclosures of purpose and intent that are necessary for the efficient detection of use and dissemination violations. This absence of disclosure then sharply limits future privacy protection.

CONCLUSION

Overall, these data show that many people value biometric privacy, and that their concerns are not motivated by a single factor. It is therefore hard to say that a truly unauthorized collection of biometric information has not caused some harm; it would have to raise none of the issues that are being cited. Though legislatures and courts may wish to exclude from protection those individuals whose biometric data is being collected with their knowledge and is only being used in ways of which they are aware, this still leaves a broad array of potential privacy harms. The immutable nature of biometrics makes it easy to repurpose biometric information collected for one purpose for other uses, and these data also show that people are extremely sensitive to this kind of purpose drift.

Given the breadth of ways in which biometrics can be used, it is easy to understand why so many people are concerned about so many possible harms. As has been noted so frequently of late in Fourth Amendment doctrine, we cannot ignore how "seismic shifts in digital technology" have challenged traditional understandings of privacy.[162] This domain is only the latest in a long line that will require policymakers to reconsider privacy standards and account for new social realities.

162. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

APPENDIX

Demographics of the sample

	First Study		Second Study		Census[162]
% Female	50.3		50.6		50.8
% Male	49.5		48.9		49.2
% Other	.2		.5		
Age (years)					
Median	45		46		
Mean	45.72	(17.05)	45.64	(16.83)	
Political Orientation (1–7)[163]					
Economic	4.12	(1.69)			
Social	3.87	(1.77)			
Overall	4.02	(1.66)	4.07	(1.73)	
Race/Ethnicity (%)					
White	77.2		76.2		76.6
Black or AA	12.8		13.0		13.4
Indian or Native	.9		1.2		1.3
SE Asian	5.9		6.1		5.8
Hawaiian/Pacific	.4		.6		.2
Multiracial or Other	2.8		2.9		2.7
Hispanic (%)	17.1		18.2		18.1
Education					
Less than HS	10.8		10.7		11.0
HS Diploma/GED	28.7		28.9		28.9
Two-Year College	29.0		29.7		28.6
Four-Year College	20.2		20.2		20.0
Graduate Degree	11.3		10.5		11.4

Note: For age and political orientation, the numbers in parentheses represent standard deviations. Hispanic identity was assessed in a separate question.

Comfort with Fingerprint and Facial Recognition Biometrics.[163]

Introductory text: Companies are increasingly collecting biometric information about their customers. The two types of information that companies most frequently collect are scans of facial geometry and fingerprints. Companies can use this information in a variety of ways. A store might use fingerprints to track participation in a discount program, with a customer scanning their finger rather than swiping a card. Or a coffee shop might use facial recognition to identify customers as they enter the shop to suggest favorite orders.

For fingerprint biometrics, a computer measures the characteristics of a person's fingertips and generates a numeric expression of each finger's unique features.

How comfortable are you with a company having a record of your fingerprints if they are free to share that information with whomever they want?
Very Uncomfortable (1) – Very Comfortable (6)

Facial geometry is somewhat like a fingerprint for the face. A computer measures the characteristics of a person's face and generates of a numeric expression of its unique features. For example, it might note the distance between a person's eyes or the width of their nose relative to their mouth.

How comfortable are you with a company having a record of your facial geometry if they are free to share that information with whomever they want?
Very Uncomfortable (1) – Very Comfortable (6)

Biometric uses for second data collection.

- A bank uses a customer's fingerprint rather than a password to access the bank's smartphone app.
- A credit card company using a voiceprint to confirm the identity of a customer when they call about their account.
- A "smart" doorbell that uses facial recognition to notify a homeowner when particular people approach their front door.
- A package pickup company that allows you to use your fingerprint to unlock the locker containing your package.
- A performance venue using facial recognition to search a crowd for known stalkers of a performer.
- A smartphone using facial recognition rather than passcodes to unlock.

163. To avoid redundancy the many versions of the main vignettes are not reprinted here. They are available from the author upon request.

- A smartphone using fingerprints rather than passcodes to unlock.
- A department store like Walmart or Home Depot using facial recognition to detect when people who have been banned from their stores - for example, people caught shoplifting - have entered.
- A department store . . . to track where individual customers go in their stores and what items those customers look at so they can later send those customers targeted advertisements.
- A program that uses facial recognition to comb social media for photos of celebrities to track their online mentions and physical locations.
- A people search company using facial recognition to link the profiles of people across different social media sites.
- A technology company using facial recognition to identify unknown persons in uploaded photos.
- A technology company using facial recognition to track people's locations using publicly uploaded photos.
- A homeowner's association using facial recognition to track the movements of people on its streets and sidewalks.
- A technology company using facial recognition to detect when photographs of its users are uploaded onto other companies' websites.
- An employer using fingerprint scans rather than timecards for people to check in at work.
- 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.
- A gym having their members check-in using a fingerprint scan rather than an id card.