BIPA: The Most Important Biometric Privacy Law in the US?

Woodrow Hartzog (Northeastern University)

In May 2020, Clearview AI abruptly ended all service contracts with all non-law enforcement entities based in Illinois.[1] The reason? It hoped to avoid an injunction and potentially large damages under one of the most important privacy laws in America: the Illinois Biometric Information Privacy Act (BIPA).[2]

Enacted in 2008 in the wake of the bankruptcy of a high-profile fingerprint-scan system, lawmakers designed BIPA to provide "safeguards and procedures relating to the retention, collection, disclosure, and destruction of biometric data."[3] It was the first state law in the US to specifically regulate biometrics. Remarkably, as the bill was being deliberated by the Illinois legislature, "there were no questions or discussion, and the bill proceeded immediately to a vote and unanimously passed in the House."[4]

BIPA's substantive rules follow a traditional approach to data protection. Compared to omnibus and complex data-protection laws like GDPR, BIPA's rules are simple. Private entities must get

1 Clearview AI scraped billions of images of people without their permission from social media websites to power their facial recognition app. Clearview filed legal documents in Illinois stating that "Clearview is cancelling the accounts of every customer who was not either associated with law enforcement or some other federal, state, or local government department, office, or agency." See Ryan Mac, Caroline Haskins, and Logan McDonald, "Clearview AI Has Promised to Cancel All Relationships with Private Companies," *BuzzFeed*, May 7, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies.

2 740 Ill. Comp. Stat. Ann. 14/15.

3 Charles N. Insler, How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act, 43 S. Ill. U. L.J. 819, 820 (2019).

4 Anna L. Metzger, The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy, 50 Loy. U. Chi. L.J. 1051, 1063 (2019).

informed consent before collecting or disseminating a person's biometric information.[5] They are prohibited from selling, leasing, trading, or otherwise profiting from a person's biometric information.[6] Companies must also follow specific retention and destruction guidelines.[7] Finally, the statute binds private entities to a standard of care in transmitting, storing, and protecting biometric information that is equal to or more protective than for other confidential and sensitive information.[8]

While other states such as Texas and Washington have passed standalone biometrics laws,[9] BIPA is the only biometric privacy law in the United States with a private cause of action. Multiple states require notice and consent before parties can collect biometric identifiers, require reasonable security measures for covered information, restrict the disclosure of biometric identifiers to specific circumstances, and limit companies' retention of biometric identifiers. But only in Illinois can people who have been aggrieved by companies that violated the rules bring their own action against the alleged violation instead of waiting for the government to file a complaint or levy a penalty.

Given the limited scope of biometric laws, BIPA's private cause of action might not seem monumental—yet it is revelatory in how is has distinguished itself from other biometrics laws. For example, Texas and Washington both authorize their state attorneys general to enforce their biometric privacy laws in ways similar to how states enforce their general data-privacy rules.[10] In contrast, BIPA's private cause of action has meaningfully shaped the practices of companies who deploy biometrics. It has also forced judges to resolve longstanding issues of injury and standing for privacy violations, among the most vexing issues for all privacy-related claims by plaintiffs in civil courts.

Plaintiffs alleging privacy-related harms from things like data breaches, abusive surveillance, and unauthorized disclosure have had a notoriously difficult time in court. Some of this is attributable to the general erosion of access to the American court system through tort reform. Plaintiffs struggle to certify classes for mass litigation, and arbitration clauses are embedded in the ubiquitous terms-of-use agreements online. But a huge roadblock for plaintiffs is the slippery nature of privacy harms.[11] Courts have long been skeptical of emotional and reputational

---

5 740 Ill. Comp. Stat. Ann. 14/15 ("§15(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it [informs the subject what is being collected and receives a written release]… .§15(c) (d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless [the subject of the biometric identifier or biometric information consents or disclosure is required pursuant to a valid warrant or subpoena]."

6 Id. § 15(c).

7 Id. § 15(a). ("A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.").

8 Id. § 15(e).

9 Tex. Bus. & Com. Code §503.001; Wash. Rev. Code Ann. §19.375.020; California Consumer Privacy Act (CCPA); N.Y. 2019 Stop Hacks and Improve Electronic Data Security (SHIELD) Act (broadening information covered by data breach response law to include biometric information); N.Y. Lab. Law §201-a (prohibiting fingerprinting as a condition of employment); Arkansas Code §4-110-103(7) (amending data breach response law to include biometric information).

10 For more information on the role of state attorneys general in privacy policymaking, see Danielle Keats Citron, The Privacy Policymaking of State Attorneys General, 92 Notre Dame L. Rev. 747, 748 (2016).

11 M. Ryan Calo, The Boundaries of Privacy Harm, 86 IND. L.J. 1131, 1133 (2011); Daniel Solove and Danielle Citron, Risk and Anxiety: A Theory of Data Breach Harms, 96 Texas Law Review 737 (2018); Ryan Calo, Privacy Harm Exceptionalism, 12 J. TELECOMM. & HIGH TECH. L. 361, 361, 364 (2014); Paul Ohm, Sensitive Information, 88 S. CAL. L. REV. 1125, 1196 (2015).

damages absent a more obvious physical or financial harm.[12] The Federal Trade Commission, the premier privacy regulator in the US, creates waves when it even hints at the idea that something more than physical or financial harm or extreme emotional suffering should be considered in determining whether particular acts are unfair.[13] This is to say nothing of the high-stakes debate over whether less specific harms such as anxiety and exposure to risk of data abuses, standing alone, can constitute an actionable injury in the context of claims of negligence which led to a data breach.[14]

But most discrete and individual privacy encroachments are not catastrophic. The modern privacy predicament is more akin to death by a thousand cuts. Small intrusions and indiscreet disclosures could lead to compromised autonomy, obscurity, and trust in relationships. What's more, it can be difficult to specifically articulate and identify the ways in which data breaches make us more vulnerable. Torts require a clear line of causation from fault to harm. That's usually relatively easy to prove with things like physical injuries from car wrecks, though it is less so with data breaches. Even if it's clear that a malicious actor has gained access to peoples' information, criminals don't always straightforwardly use data obtained from a breach to inflict direct financial or emotional injury upon the data subject. They often aggregate the information in a pool for further exploitation or sit on it for years so as not to arouse suspicion. Often people have no idea who wronged them online. American data-privacy law simply isn't built to respond to this kind of diffuse and incremental harm.[15]

BIPA has spurred a key intervention into this morass. Specifically, with BIPA, several judicial opinions have affirmed the argument that regardless of whether wrongful acts with biometric information resulted in chilling effects or financial or emotional injury, the collection and processing of biometric data without notice and consent is alone a cognizable injury because it is an affront to a person's dignity and autonomy. Two cases in particular demonstrate the importance of BIPA.

In *Rosenbach v. Six Flags Entm't Corp.*, a mother brought a claim on behalf of her son against Six Flags amusement park for the company's failure to give notice or obtain consent when collecting the child's fingerprints for their biometric identification system.[16] At issue was whether the plaintiffs alleged sufficient actual or threatened injury to have standing to bring suit. Plaintiffs did not allege financial or extreme emotional harm, but rather a harm resulting solely from the prohibited collection and processing of personal biometric data without making the required

---

12 Id.

13 See F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 623 (D.N.J. 2014), aff'd, 799 F.3d 236 (3d Cir. 2015) ("The parties contest whether non-monetary injuries are cognizable under Section 5 of the FTC Act….Although the Court is not convinced that non-monetary harm is, as a matter of law, unsustainable under Section 5 of the FTC Act, the Court need not reach this issue….").

14 Daniel Solove and Danielle Citron, Risk and Anxiety: A Theory of Data Breach Harms, 96 Texas Law Review 737 (2018).

15 Daniel J. Solove and Danielle Keats Citron, Risk and Anxiety: A Theory of Data-Breach Harms, 96 Tex. L. Rev. 737, 762 (2018) ("Hackers may not use the personal data in the near term to steal bank accounts and take out loans. Instead, they may wait until an illness befalls a family member and then use personal data to generate medical bills in a victim's name. They may use the personal data a year later but only use some individuals' personal information for fraud.").

16 Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 8, 129 N.E.3d 1197, 1200–01 ("The complaint alleges that this was the first time Rosenbach learned that Alexander's fingerprints were used as part of defendants' season pass system. Neither Alexander, who was a minor, nor Rosenbach, his mother, were informed in writing or in any other way of the specific purpose and length of term for which his fingerprint had been collected. Neither of them signed any written release regarding taking of the fingerprint, and neither of them consented in writing 'to the collection, storage, use sale, lease, dissemination, disclosure, redisclosure, or trade of, or for [defendants] to otherwise profit from, Alexander's thumbprint or associated biometric identifiers or information.'").

disclosures or obtaining written consent. The Appellate Court of Illinois held that "a plaintiff is not 'aggrieved' within the meaning of the Act and may not pursue either damages or injunctive relief under the Act based solely on a defendant's violation of the statute. Additional injury or adverse effect must be alleged."[17] However, the Supreme Court of Illinois disagreed.

Chief Justice Lloyd A. Karmeier, writing the opinion of the court, noted that if the Illinois legislature had wanted to impose an injury requirement beyond disclosure and consent failures, they likely would have done so, as they have in other legislation.[18] Using accepted principles of statutory construction, the court interpreted BIPA's language that "[a]ny person aggrieved by a violation of this Act shall have a right of action" according to its commonly understood legal meaning. Specifically, they found that "to be aggrieved simply 'means having a substantial grievance; a denial of some personal or property right.'"[19] Justice Karmeier wrote, "A person who suffers actual damages as the result of the violation of his or her rights would meet this definition of course, but sustaining such damages is not necessary to qualify as 'aggrieved.'"[20]

The court in *Rosenbach* found that Six Flags violated BIPA's "right to privacy in and control over their biometric identifiers and biometric information."[21] BIPA's disclosure and consent requirements give shape to that right. Thus, if a company violates BIPA, then the data subject is legally "aggrieved" because their right to privacy in and control over their biometric data has been compromised.[22]

Perhaps the most significant passage in *Rosenbach* concerned the court's response to the defendant's argument that its BIPA violations were merely "technical" in nature. The court argued that such a characterization misunderstands not only what the legislature was trying to accomplish but also the unique nature of how biometrics threaten peoples' privacy and how procedural rules mitigate that threat. "The Act vests in individuals and customers the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent."[23] Peoples' unique biometric identifiers, now easily wholesale collected and stored, are not like other kinds of authenticators like passwords and social security numbers because if they are compromised, they cannot be changed. Even beyond identity theft, the court noted that biometrics are particularly concerning because their full risks are not known. The court was direct in its finding:

---

17 Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 15, 129 N.E.3d 1197, 1202 (citing Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, rev'd, 2019 IL 123186, 129 N.E.3d 1197).

18 Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 25, 129 N.E.3d 1197, 1204. ("Defendants read the Act as evincing an intention by the legislature to limit a plaintiff's right to bring a cause of action to circumstances where he or she has sustained some actual damage, beyond violation of the rights conferred by the statute, as the result of the defendant's conduct. This construction is untenable. When the General Assembly has wanted to impose such a requirement in other situations, it has made that intention clear.").

19 Id. (citing Glos v. People, 259 Ill. 332, 340, 102 N.E. 763 (1913)).

20 Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 30, 129 N.E.3d 1197, 1205 ("Rather, '[a] person is prejudiced or aggrieved, in the legal sense, when a legal right is invaded by the act complained of or his pecuniary interest is directly affected by the decree or judgment.'") (citing Glos v. People, 259 Ill. 332, 340, 102 N.E. 763 (1913)).

21 Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206.

22 Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206 ("No additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action.").

23 Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 34, 129 N.E.3d 1197, 1206.

> When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, "the 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."...This is no mere "technicality." The injury is real and significant.[24]

The court also highlighted how integral a private cause of action was in implementing the legislature's privacy goals for BIPA. When companies face liability for legal violations without burdening plaintiffs to show some additional injury, "those entities have the strongest possible incentive to conform to the law and prevent problems before they occur and cannot be undone."[25] The court noted that the cost of complying with BIPA is "likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded; and the public welfare, security, and safety will be advanced."[26] According to the court, to force plaintiffs to wait until they could prove some sort of financial or emotional harm would counteract BIPA's prevention and deterrence goals.

The other case illustrative of BIPA's potency, *Patel v. Facebook*,[27] involves federal standing doctrine as required by Article III of the US Constitution, a concept linked to injury and harm thresholds. Standing doctrine requires that plaintiffs "must have suffered an 'injury in fact'—an invasion of a legally protected interest which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical."[28] In a landmark 2016 US Supreme Court case, *Spokeo, Inc. v. Robins* affirmed that an injury-in-fact for information-related complaints like those against data brokers for mishandling, inaccuracies, and indiscretion must be "concrete," though the court was frustratingly vague about what kinds of harms met that threshold.[29]

Patel v. Facebook involved a complaint that Facebook violated BIPA with its use of facial recognition tools. The Ninth Circuit applied a two-part test to determine "(1) whether the statutory provisions at issue were established to protect [the plaintiff's] concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests."[30] The Ninth Circuit answered yes to both questions.

In determining that BIPA protected a concrete interest rather than a purely procedural protection, the Ninth Circuit noted that privacy rights have long served as the basis for legal action in the common law, constitutional law, and in statues at both the state and federal level. The court noted the significant vulnerabilities created by facial recognition technology:

---

24 Id.

25 Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 37, 129 N.E.3d 1197, 1206.

26 Id.

27 Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019), cert. denied, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020).

28 Lujan v. Defs. of Wildlife, 504 U.S. 555, 561, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992).

29 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548–49, 194 L. Ed. 2d 635 (2016), as revised (May 24, 2016). ("When we have used the adjective 'concrete,' we have meant to convey the usual meaning of the term—'real,' and not 'abstract.'...Concreteness, therefore, is quite different from particularization. 'Concrete" is not, however, necessarily synonymous with 'tangible.' Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.") The Court went on to muddy the waters in Spokeo even further, writing, "Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, [Plaintiff] could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III...This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness." *Id* at 1549.

30 Patel v. Facebook, Inc., 932 F.3d 1264, 1270–71 (9th Cir. 2019), cert. denied, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020) (citing Robins v. Spokeo, Inc., 867 F.3d 1108, 1113 (9th Cir. 2017) (Spokeo II)).

> [T]he facial-recognition technology at issue here can obtain information that is "detailed, encyclopedic, and effortlessly compiled," which would be almost impossible without such technology...Once a face template of an individual is created, Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location. Facebook can also identify the individual's Facebook friends or acquaintances who are present in the photo...[It] seems likely that a face-mapped individual could be identified from a surveillance photo taken on the streets or in an office building. Or a biometric face template could be used to unlock the face recognition lock on that individual's cell phone.[31]

The court concluded that "the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests. Similar conduct is actionable at common law."[32] The court cited the language in Rosenbach in holding that "'the statutory provisions at issue' in BIPA were established to protect an individual's 'concrete interests' in privacy, not merely procedural rights," and that by alleging a BIPA violation the "the plaintiffs have alleged a concrete injury-in-fact sufficient to confer Article III standing.[33]

BIPA has a number of virtues. Thanks to BIPA's private cause of action, it has become the key for holding companies that use biometric systems accountable.[34] In the absence of a private cause of action, enforcement of biometrics and consumer protection laws is generally left to state attorneys general (AG). While state AGs are certainly key to privacy policymaking in the US, they have limited resources and a host of issues on their plate.[35] Even with unlimited bandwidth, state AGs have limited legal ability and political capital to extract the kind of fines necessary to sufficiently deter companies. The same holds true for the Federal Trade Commission, which is America's primary privacy regulator.[36]

So far, only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses. Regulators are more predictable than plaintiffs and are vulnerable to political pressure. Facebook's share price actually rose 2 percent after the FTC announced its historic $5 billion fine for the social media company's privacy lapses in the Cambridge Analytica debacle.[37] Meanwhile, Clearview AI specifically cited BIPA as the reason it is no longer pursuing non-government contracts.[38] On top of that, Clearview AI is being sued by the ACLU for violating

---

31 Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019), cert. denied, 140 S. Ct. 937, 205 L. Ed. 2d 524 (2020) (citations omitted). BIPA's focus on face templates as a creation that grants surveillance and other affordances is properly distinguished from a standard photograph, which does not provide the same affordance of serving as a beacon.

32 Id.

33 Id. at 1274.

34 Over three hundred class action lawsuits have been brought under BIPA as of June 2019. See Seyfarth Shaw, "Biometric Privacy Class Actions by the Numbers: Analyzing Illinois' Hottest Class Action Trend," Seyfarth, June 28, 2019, https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/.

35 See Danielle Keats Citron, The Privacy Policymaking of State Attorneys General, 92 Notre Dame L. Rev. 747 (2016).

36 See Daniel Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia Law Review 583 (2014); Woodrow Hartzog and Daniel Solove, The Scope and Potential of FTC Data Protection, 83 George Washington Law Review 2230 (2015).

37 Charlotte Jee, "Facebook Is Actually Worth More Thanks to News of the FTC's $5 Billion Fine," MIT Technology Review, July 15, 2019, https://www.technologyreview.com/2019/07/15/134196/facebook-is-actually-richer-thanks-to-news-of-the-ftcs-5-billion-fine/.

38 Nick Statt, "Clearview AI to Stop Selling Controversial Facial Recognition App to Private Companies," *Verge*, May 7, 2020, https://www.theverge.com/2020/5/7/21251387/clearview-ai-law-enforcement-police-facial-recognition-illinois-privacy-law.

BIPA by creating faceprints of people without their consent.[39] It is no wonder that the private cause of action is one of two reasons the United States does not have an omnibus federal data privacy law (the other being federal preemption of state privacy frameworks).[40] In general, businesses have opposed private causes of action more than other proposed privacy rules, short of an outright ban.[41]

Even given BIPA's virtues and remarkable effectiveness, it is probably not the best model for America's biometric privacy identity. A private cause of action is necessary, but not sufficient, to respond to the risk of biometrics. BIPA is rooted in a myopic and atomistic "notice and choice" approach to privacy.

There are two major problems with building a biometric privacy framework almost exclusively around concepts of transparency and informational self-determination. First, by focusing on giving people control over their data and mandating procedural disclosure obligations, these frameworks fail to impose substantive limits on how far companies can encroach into our lives and how deeply these systems can be entrenched. Procedural transparency and consent regimes end up serving as a justification mechanism for all kinds of encroachments without any clear backstop to how vulnerable we can be made to these systems, so long as we consent. Furthermore, BIPA fails to address the issues around privacy in public spaces or in data that already has been exposed to the public. For example, judges considering privacy claims have said repeatedly that "there can be no privacy in that which is already public."[42]

Privacy is about more than just informational self-determination. It is about trust, dignity, freedom from oppression, and laying the preconditions for human flourishing. But those values are not necessarily reflected in the net outcome of billions of individual decisions. Moreover, companies create structured environments that can heavily influence these discrete choices, with powerful incentives to get us to say "yes" any way they can.[43]

---

39 ACLU, American Civil Liberties Union, American Civil Liberties Union of Illinois, Chicago Alliance Against Sexual Exploitation, Sex Workers Outreach Project Chicago, Illinois State Public Interest Research Group, Inc., and Mujeres Latinas en Acción v. Clearview AI, Inc., https://www.aclu.org/sites/default/files/field_document/aclu_v_clearview_complaint_final.pdf.

40 See Makena Kelly, "Congress Is Split over Your Right to Sue Facebook," *Verge*, December 3, 2019, https://www.theverge.com/2019/12/3/20993680/facebook-google-private-right-of-action-sue-data-malpractice-wicker-cantwell; and Emily Birnbaum, "Lawmakers Jump-Start Talks on Privacy Bill," The Hill, August 7, 2019, https://thehill.com/policy/technology/456459-lawmakers-jump-start-talks-on-privacy-bill; and Ben Kochman, "Senate Privacy Hearing Zeroes in on Right to Sue, Preemption," *Law360*, December 4, 2019 (paywall), https://www.law360.com/articles/1224809/senate-privacy-hearing-zeroes-in-on-right-to-sue-preemption; and Cameron F. Kerry, John B. Morris, Caitlin Chin, and Nicol Turner Lee, "Bridging the Gaps: A Path Forward to Federal Privacy Legislation," *Brookings*, June 3, 2020, https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation/.

41 See Issie Lapowsky, "New York's Privacy Bill Is Even Bolder than California's, Wired, June 4, 2019, https://www.wired.com/story/new-york-privacy-act-bolder/; DJ Pangburn, "How Big Tech Is Trying to Shape California's Landmark Privacy Law," *Fast Company*, April 25, 2019, https://www.fastcompany.com/90338036/how-big-tech-is-trying-to-shape-californias-landmark-privacy-law; John Hendel and Cristiano Lima, "Lawmakers Wrangle over Consumer Lawsuits as Privacy Talks Drag," *Politico*, June 5, 2019, https://www.politico.com/story/2019/06/05/privacy-advocates-consumer-lawsuits-1478824; and "Potentially Expanded Private Right of Action Increases Risk of Class Action Exposure under the California Consumer Privacy Act," *Dorsey*, May 1, 2019, https://www.dorsey.com/newsresources/publications/client-alerts/2019/04/private-right-of-action-increases-risk.

42 Woodrow Hartzog, The Public Information Fallacy, 98 Boston University Law Review 459 (2019). The FBI alleges it does not need permission to conduct surveillance using powerful technologies like cell-site simulators (often called "Stingrays"), so long as they are doing so in public places. Judges have refused to punish people for taking "upskirt" photos because the women photographed have no reasonable expectation of privacy "in public," no matter how fleeting their exposure. *Id*.

43 Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, MA: Harvard University Press, 2018).

BIPA is simply not capable of providing individuals with meaningful agency over modern data practices.[44] "Informed consent" is a broken privacy regulatory mechanism.[45] It doesn't scale, it offloads risk onto the person giving the consent, and it is easily manufactured by companies who control what we see and what we can click. Companies deploy malicious user interfaces and a blizzard of dense fine print to overwhelm our decision-making process. Consent regimes give the illusion of control while justifying dubious practices that people don't have enough time or cognitive resources to understand. Even if people were able to adequately gauge the risks and benefits of consenting to biometric practices, they often don't have a meaningful choice in front of them since they cannot afford to say no and decline a transaction or relationship. While people should be protected regardless of what they consent to, BIPA is largely agnostic to the post-permission risks of biometric technologies.

BIPA is far more effective than any other law on the books in protecting our biometric privacy with respect to private companies. However, it does not confront the structural change and substantive limits necessary for a sustainable future with biometric technologies. BIPA allows companies to exploit people as their consent is harvested through systems designed to have them hurriedly click "I Agree" and get on with their busy lives. BIPA's success entrenches an overly individualistic and procedural approach to privacy, but has shown lawmakers what is indispensable in a biometric privacy framework. It is a guide not just because of what it provides but also because of what it lacks.

44 Woodrow Hartzog, The Case Against Idealising Control, 4 European Data Protection Law Review 423 (2018).

45 Neil Richards and Woodrow Hartzog, The Pathologies of Digital Consent, 96 Washington University Law Review 1461 (2019); Evan Selinger and Woodrow Hartzog, The Inconsentability of Facial Surveillance, 66 Loyola Law Review 101 (2019).