St. John's Law Review

Volume 94
Number 3 *Volume 94, Fall 2021, Number 3*

Article 8

Closing the Data Gap: Protecting Biometric Information Under the Biometric Information Privacy Act and the California Consumer Protection Act

Eva-Maria Ghelardi

CLOSING THE DATA GAP: PROTECTING BIOMETRIC INFORMATION UNDER THE BIOMETRIC INFORMATION PRIVACY ACT AND THE CALIFORNIA CONSUMER PROTECTION ACT

EVA-MARIA GHELARDI[†]

INTRODUCTION

Between May and June of 2014, Stacy Rosenbach bought her son, Alexander, a Six Flags season pass online.[1] She submitted Alexander's personal information and read that Alexander would complete the sign-up process at the park.[2] No details described what the sign-up process would entail.[3]

After showing his online receipt at Six Flags, Alexander was brought to an office to provide the customary thumb scan.[4] Alexander's thumb scan, along with the season pass card, was required to permit him to enter the various rides.[5] He was not given any information about how his thumb scan would be stored or used after his season pass expired.[6] Alexander—a fourteen-year-old boy—thought nothing of this process and voluntarily gave Six Flags his thumb scan.[7]

Mrs. Rosenbach, on the other hand, was shocked to learn of this scan when Alexander returned home.[8] After Mrs. Rosenbach asked Alexander for the paperwork from the season pass, he told her Six Flags "did 'it all by fingerprint now.' "[9] Although Alexander never returned to Six Flags, Six Flags kept his biometric

---

[†] Senior Staff, *St. John's Law Review*, J.D. Candidate, 2021, St. John's University School of Law; M.A., 2015, Columbia University; B.A., 2014, The Catholic University of America.

[1] Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶ 5.

[2] *Id.*

[3] *Id.* ¶¶ 5, 8.

[4] *Id.* ¶ 6.

[5] *Id.*

[6] *Id.* ¶ 8.

[7] *Id.* ¶¶ 6–7.

[8] *Id.* ¶ 8.

[9] *Id.* ¶ 7.

information.[10] Curiously, Six Flags has not revealed how long it planned to keep Alexander's thumb scan or how it planned to use it.[11]

Despite their concerns, the Rosenbachs were protected by the country's strongest biometric information privacy law.[12] In 2009, Illinois was the first state to regulate certain uses of "biometric information" and "biometric identifier[s]" with the Biometric Information Privacy Act ("BIPA").[13] Under BIPA, "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" are biometric identifiers.[14] BIPA defines biometric information as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[15] A thumb scan, like the one Six Flags took of Alexander, is therefore a biometric identifier, and its codified and stored counterpart is biometric information.

Concerns of indiscriminate use of collected biometric information during the Pay By Touch bankruptcy prompted BIPA's enactment in 2008.[16] At the time, Pay By Touch "operat[ed] the largest fingerprint scan system in Illinois."[17] Its pilot program promised to make payment more efficient by linking financial information like "credit cards, bank accounts, [and] rewards programs" to biometric information.[18] Millions of Illinoisans

---

[10] *Id.* ¶ 9.

[11] *Id.*

[12] Kathryn Leicht, *The Future of Biometric Data Privacy Law and BIPA*, N.Y.U. J. INTELL. PROP. & ENT. L.: THE BLOG (Mar. 7, 2019), https://blog.jipel.law.nyu.edu/2019/03/the-future-of-biometric-data-privacy-law-and-bipa/ [https://perma.cc/BMM4-AJ23].

[13] 740 ILL. COMP. STAT. ANN. 14/10 (West 2010).

[14] *Id.* The statute lists a variety of exceptions to the biometric identifier definition including

> writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, . . . physical descriptions such as height, weight, hair color, or eye color[,] . . . donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency.

Id.

[15] *Id.*

[16] Annemaria Duran, *Understanding The Illinois Biometric Information Privacy Act & Its Relation to Employers*, SWIPECLOCK, (Dec. 27, 2017), https://www3.swipeclock.com/blog/understanding-illinois-biometric-information-privacy-act-relation-employers/ [https://perma.cc/B8AR-3S8J].

[17] Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, ILL. BAR J., Mar. 2018, at 34, 35.

[18] Duran, *supra* note 16.

signed up and used Pay By Touch in cooperating "grocery stores, gas stations, and school cafeterias."[19] When Pay By Touch declared bankruptcy in 2008, many were concerned that their biometric information would be sold as assets of the bankrupt company[20] because no federal laws protected individuals' biometric information from being commodified for financial use.[21]

To address these fears, the Illinois Legislature enacted BIPA.[22] BIPA requires individuals (1) to receive notice of the collection or storage of biometric information or identifiers, (2) to receive notice of the purpose and time span of such collection or storage, and (3) to give written consent to the process.[23]

Not only did BIPA protect Alexander's thumb scan, but it also provided the Rosenbachs with a private cause of action for any statutory violations by Six Flags.[24] BIPA required notice, oversight, and regulation of the collected personal information.[25]

Since Six Flags did not provide Alexander with the required information during his sign-up process, Stacy Rosenbach—acting as mother and legal representative of Alexander—filed a BIPA claim against Six Flags Entertainment Corporation in the circuit court of Lake County, seeking redress for Alexander and other similarly situated persons.[26]

While *Rosenbach* moved through the Illinois court system, California spearheaded the country's "most comprehensive" biometric information law.[27] The California Consumer Privacy Act ("CCPA") provided a new gloss on BIPA when it went into effect on January 1, 2020.[28] Although fifteen states proposed similar laws, many observers expected CCPA to act as the new national

---

[19] *Id.*; Insler, *supra* note 17.

[20] Insler, *supra* note 17.

[21] *Biometric Security Poses Huge Privacy Risks*, SCI. AM. (Jan. 1, 2014), https://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks/ [https://perma.cc/TZU9-UCF9].

[22] Duran, *supra* note 16.

[23] 740 ILL. COMP. STAT. ANN. 14/15(b)(1)–(b)(3) (West 2010).

[24] Leicht, *supra* note 12.

[25] DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 2 (2011).

[26] Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶¶ 1, 10.

[27] Stuart D. Levi & Daniel Healow, *California Consumer Privacy Act: A Compliance Guide*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES (Mar. 20, 2019), https://www.skadden.com/insights/publications/2019/03/california-consumer-privacy-act [https://perma.cc/GJ9S-Z8RA].

[28] *Id.*; Jeremy Kirk, *California's New Privacy Law: It's Almost GDPR in the U.S.*, BANK INFO SEC. (July 2, 2018), https://www.bankinfosecurity.com/californias-new-privacy-law-its-almost-gdpr-in-us-a-11149 [https://perma.cc/VF26-VMJA].

baseline for biometric information privacy, given California's size and its economic importance.[29] Most tech companies are based in Silicon Valley,[30] and few companies were expected to maintain separate frameworks for each state's regulations.[31] Those familiar with the industry predicted that companies affected by the new regulation would provide CCPA-level protection to "all their U.S. customers," but instead most companies have opted to afford CCPA's broad protections only to Californians.[32] To achieve the desired nationwide level of protection, individual states must therefore continue to move ahead with their own laws.

CCPA grants consumers "more information [about] and control over" their biometric information through the right to general disclosure, specific requests for information, deletion, and "equal service and pricing."[33] Violations give rise to standing for "consumers."[34] Given the hefty fines imposed for violating the statute, businesses will likely interpret "consumers" broadly to avoid inadvertent violations.[35]

Similar to BIPA, the CCPA arose out of public concern about the new almost "limitless natural deposit" of personal information collected and refined for a valuable profit-driven

---

[29] *See* Zack Whittaker, *Silicon Valley Is Terrified of California's Privacy Law. Good*, TECHCRUNCH (Sept. 19, 2019, 12:00 PM), https://techcrunch.com/2019/09/19/silicon-valley-terrified-california-privacy-law/ [https://perma.cc/A45F-U9NC]. Hawaii, Massachusetts, New Jersey, Pennsylvania, Rhode Island, and even Puerto Rico proposed bills similar to CCPA. George P. Slefo, *Bracing for Sweeping New Data Privacy Law*, ADAGE (Oct. 14, 2019), https://adage.com/article/news/how-brands-are-preparing-californias-privacy-act-becomes-reality-2020/2205586 (subscription required). Twenty seven states are developing new privacy laws, although not all of them are similar to CCPA. *See id.*; *see also* Juliana De Groot, *What Is the California Consumer Privacy Act?*, DIGITAL GUARDIAN (July 15, 2019), https://digitalguardian.com/blog/what-california-data-privacy-protection-act [https://perma.cc/3LZ6-RM6H]. *See generally* Levi & Healow, *supra* note 27.

[30] Slefo, *supra* note 29.

[31] *Id.*

[32] Patience Haggin, *Businesses Across the Board Scramble To Comply with California Data-Privacy Law*, WALL ST. J. (Sept. 8, 2019, 9:00 AM), https://www.wsj.com/articles/businesses-across-the-board-scramble-to-comply-with-california-data-privacy-law-11567947602 [https://perma.cc/R8Z9-7QEC]; *Amazon and Your Data*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=G68RWEYX26H3ZXJT [https://perma.cc/MEB8-NDLW] (last visited Mar. 20, 2021); *Walmart Privacy Policy*, WALMART, https://corporate.walmart.com/privacy-security/walmart-privacy-policy [https://perma.cc/75UN-AT3N] (last updated July 1, 2020).

[33] Levi & Healow, *supra* note 27; De Groot, *supra* note 29.

[34] CAL. CIV. CODE § 1798.140(o)(1)(E) (West 2020).

[35] Levi & Healow, *supra* note 27.

market.[36] An estimated $12 billion worth of personal information is used for advertising in California each year.[37] Every industry exploited this data, yet California consumers had no legal protections.[38]

Part I of this Note examines the *Rosenbach* case's interpretation and application of Illinois's BIPA as well as the gaps left by the decision. Part II examines how the upcoming CCPA addresses these issues. Part III examines gaps that remain despite the overlap between BIPA and CCPA. Finally, Part IV recommends methods that courts and legislatures could use to promote the legislative intent behind BIPA and CCPA by filling gaps and extending existing protections to newly evolving technologies and threats.

I. BIPA PROTECTIONS AFTER *ROSENBACH*

A. BIPA Cases Before Rosenbach

Before the *Rosenbach* decision, Illinois courts dismissed over 150 BIPA suits for lack of "actual injury or adverse effect," meaning plaintiffs had failed to prove that they suffered a financial or other injury.[39] BIPA did not explicitly mention standing, and the courts reasoned that the federal constitutional standing requirement also applied to BIPA claims.[40]

---

[36] Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—and Won*, N.Y. TIMES MAG. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html [https://perma.cc/CEZ6-YFHW].

[37] Lauren Feiner, *California's New Privacy Law Could Cost Companies a Total of $55 Billion To Get in Compliance*, CNBC (Oct. 8, 2019, 10:38 AM), https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html [https://perma.cc/5UQP-D4CS].

[38] Brenda Stoltz, *A New California Privacy Law Could Affect Every U.S. Business—Will You Be Ready?*, FORBES (Sept. 7, 2019, 7:52 PM), https://www.forbes.com/sites/allbusiness/2019/09/07/california-consumer-privacy-act-could-affect-your-business/#488236cb36ac [https://perma.cc/Q26U-F3LW]; Confessore, *supra* note 36.

[39] Gerald L. Maatman, Jr., et al., *Biometric Privacy Class Actions by the Numbers: Analyzing Illinois' Hottest Class Action Trend*, SEYFARTH SHAW LLP: WORKPLACE CLASS ACTION BLOG (June 28, 2019), https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/ [https://perma.cc/7NVY-A82R]; Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶ 1.

[40] *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (holding plaintiffs must have "concrete and particularized" injuries to have standing in federal court). Injuries must be immediate and have a direct stake in the outcome of the appeal. *See* Hollingsworth v. Perry, 558 U.S. 183, 196 (2010). A simple violation of BIPA was, therefore, not previously considered sufficient to create standing without

The first indication of changed legislative intent came when the Illinois Legislature rejected amendment S.B. 3053 on January 9, 2019.[41] The amendment would have exempted from BIPA the gathering of biometric information collected for noncommercial reasons, or of information that was protected at least as much as other information a company stored.[42]

This rejection indicated that the Illinois Legislature wanted to hold private companies accountable for the collected biometric information regardless of the purpose, profit, or level of protection.[43] The declined amendment may have played a role in the *Rosenbach* court's interpretation of the legislative intent behind BIPA.[44] It showed that the Legislature's focus was on protecting the individual, not on categorizing specific uses of biometric information.[45]

Following this unsuccessful attempt to narrow BIPA, *Rosenbach* marked a shift in Illinois's BIPA landscape; the Illinois Supreme Court overturned nine years of Illinois precedent by granting standing to individuals whose biometric information was collected without the required notice and consent.[46] Illinois plaintiffs no longer needed to allege an actual injury under BIPA; BIPA granted consumers a say in the collection of their biometric information before a security breach occurred and the right to enforce such protections through private suits.[47]

B. Procedural History of Rosenbach

After Rosenbach filed suit, Six Flags submitted a combined motion seeking "dismissal of [the] action under both sections 2-615 and 2-619 of the [Illinois] Code."[48] Six Flags asserted that Rosenbach lacked standing as a result of suffering no actual or threatened injury.[49] After a hearing, the circuit court proceeded

---

evidence of further injury. Almost all of the 173 BIPA cases were dismissed on issues of standing. *See* Maatman et al., *supra* note 39.

[41] *See* Leicht, *supra* note 12.

[42] S.B. 3053, 100th Gen. Assemb. (Ill. 2018).

[43] *Id.*

[44] *See* Alan S. Wernick, *Biometric Information—Permanent Personally Identifiable Information Risk*, AM. BAR ASS'N (Feb. 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_8/ [https://perma.cc/B6YG-6EHK].

[45] *Id.*

[46] Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶¶ 1, 38.

[47] *Id.*

[48] *Id.* ¶ 12.

[49] *Id.*

under section 2-615 of the Code, denying the motions in part and dismissing claims in part with prejudice.[50]

Defendants then "sought interlocutory review . . . under Illinois Supreme Court Rule 308," claiming that the case involved a controversial question of law.[51] The circuit court held that Mrs. Rosenbach, on behalf of her son Alexander, had not suffered an actual injury through the collection of his biometric information.[52] Mrs. Rosenbach appealed.[53] The appellate court granted review and decided that Mrs. Rosenbach was not "aggrieved" within the meaning of BIPA and could not pursue damages or injunctive relief solely based on defendant's violation of the statute.[54]

The appellate court reasoned that the plain meaning of "aggrieved" suggests that an actual injury is still necessary.[55] Using persuasive district court decisions, the court reasoned that the Legislature could have simply written that each "technical violation" was actionable, but chose instead to say "aggrieved."[56] The Illinois Legislature, the court decided, does not act through inferences.[57] Therefore, the appellate court refused to read strict liability for violations into the statute.[58] In response, Rosenbach petitioned the Illinois Supreme Court for leave to appeal, which the court granted.[59]

C. The Rosenbach *Court's Reasoning*

The Supreme Court of Illinois properly used statutory interpretation tools, such as plain language, precedent, legislative intent, and legislative history, to find that "aggrieved by a violation" created strict liability for BIPA violations and created individual causes of action for improperly collected and stored biometric information.[60] Chief Justice Karmeier utilized the context of BIPA's enactment and the unique nature of

---

[50] *Id.* ¶ 13.

[51] *Id.* ¶ 14. Defendants also alleged there was "substantial ground for a difference of opinion." *Id.*

[52] *See id.* ¶ 15.

[53] *Id.* ¶ 16.

[54] Rosenbach v. Six Flags Ent. Corp., 2017 IL App (2d) 170317, ¶ 28 (quoting 740 ILL. COMP. STAT. ANN. 14/20 (West 2010)), *rev'd*, 2019 IL 123186.

[55] *Id.* ¶ 20.

[56] *Id.* ¶ 28.

[57] *See id.*

[58] *See id.*

[59] Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶¶ 1, 16.

[60] *Id.* ¶ 21 (quoting 740 ILL. COMP. STAT. ANN. 14/20 (West 2010)).

biometric information to inform the court's decision.[61] However, the holding brushed over important policy considerations for the purpose of making a general conclusion that would be widely applicable.

1. Textual Arguments

Under a plain meaning analysis, the Supreme Court of Illinois found a meaningful variation between "aggrieved" and "injured." Since BIPA does not contain a definition of "aggrieved," the court in *Rosenbach* applied the ordinary meaning doctrine, which would not require actual injury.[62]

The court then examined the "settled legal meaning" of "aggrieved."[63] Courts generally infer that legislatures intended settled legal meanings to guide the interpretation of the law.[64] In 1913, the Supreme Court of Illinois interpreted "aggrieved" to mean "a substantial grievance; a denial of some personal of property right."[65] According to *Glos v. People*, aggrieved should be interpreted "in the legal sense, when a legal right is invaded."[66] *Glos*'s interpretation of "aggrieved" was "repeated frequently by Illinois courts and was embedded in [Illinois] jurisprudence when [BIPA] was adopted."[67] The *Rosenbach* court then cited cases from 1943, 1958, 1973, and 2004, showing that the Legislature had notice of the legal interpretation of "aggrieved."[68] Application of *expressio unius est exclusio alterius* and the ordinary legal understanding showed the Legislature, therefore, meant for "aggrieved" to be translated differently from "injured."[69]

Next, the *Rosenbach* court looked at common dictionaries printed around 2008 to determine the "popularly understood meaning"[70] of "aggrieved" at the time BIPA was enacted. The *Merriam-Webster's Collegiate Dictionary* from 2006 "define[d] aggrieved as 'suffering from an infringement or denial of legal

---

[61] *Id.* ¶ 19.
[62] *Id.* ¶ 29.
[63] *Id.*
[64] *Id.*
[65] Glos v. People, 102 N.E. 763, 766 (Ill. 1913).
[66] *Id.*
[67] *Rosenbach*, 2019 IL 123186, ¶¶ 1, 31.
[68] *Id.* ¶ 31.
[69] *Id.* ¶ 29–32.
[70] *Id.* ¶ 29.

rights.' "[71] *Black Law's Dictionary* in 2009 defined it as "having legal rights that are adversely affected."[72] Both of these definitions from around the time of BIPA's enactment show that the popular meaning of "aggrieved" related to the infringement of legal rights, not to actual injury. The popular meaning of "aggrieved" in 2008 weighed in Rosenbach's favor.

Rosenbach affirmed that if the Legislature wanted to impose a higher burden on plaintiffs, it had to "ma[ke] that intention clear."[73] Using *exclusio unius*, the court reasoned that the Illinois Legislature knew how to explicitly require actual injuries, as it had done so in various statutes in the past.[74] Past statutes had created a private cause of action with and without requirements of actual injury.[75] Section 10a of the Consumer Fraud and Deceptive Business Practice Act clearly stated that "actual damage" must be alleged.[76] When the Legislature used "aggrieved" language, proof of "actual damage" was not required, as in the AIDS Confidentiality Act.[77] These prior statutes illustrated clear examples where the Legislature "wanted to impose such . . . requirement[s] in other situations."[78] BIPA, the court concluded, contained "terms that parallel[ed] the AIDS Confidentiality Act."[79] If the Illinois Legislature wanted courts to interpret "aggrieved" to require actual injury, it should have used clearer language to express its intentions.[80] As written, BIPA's text was more similar to statutes that did not require actual injury.[81]

The *Rosenbach* court determined that BIPA's language was clear in requiring only aggrievement by a BIPA violation, rather than an actual injury.[82] The court then complemented its textual holding with supplemental contextual support.[83]

---

[71] *Id.* ¶ 32 (quoting *Aggrieved*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2006)).
[72] *Id.* (quoting *Aggrieved*, BLACK'S LAW DICTIONARY (9th ed. 2009)).
[73] *Id.* ¶ 25.
[74] *Id.*
[75] *Id.* ¶¶ 26–27.
[76] 815 ILL. COMP. STAT. ANN. 505/10a(a) (West 2008).
[77] Doe v. Chand, 781 N.E.2d 340, 351 (Ill. App. Ct. 2002).
[78] *Rosenbach*, 2019 IL 123186, ¶ 25.
[79] *Id.* ¶ 27.
[80] *Id.* ¶ 25.
[81] *Id.* ¶¶ 29–31.
[82] *Id.* ¶ 29.
[83] *Id.* ¶ 28.

2. Contextual Arguments

According to the *Rosenbach* court, when considering the meaning of a word in a statute, courts should look to "the connection in which the word is used, the object or purpose of the statute, and the consequences which probably will result from the proposed construction."[84] The court admitted that parallel language in the AIDS Confidentiality Act is "instructive" but "not dispositive."[85] Language should be interpreted in context, but within a relevant scope.[86] After all, "[s]eparate acts with separate purposes need not . . . define similar terms in the same way."[87] The *Rosenbach* court acknowledged that each Legislature could not have a complete understanding of the ways in which a word was used throughout all federal laws, but this did not invalidate BIPA's explicit language.[88]

The *Rosenbach* court said that the appellate court misunderstood the Legislature's purpose—to prevent the compromise of sensitive biometric information.[89] The appellate court approached BIPA in a "merely 'technical' " manner[90] and thereby misinterpreted the preventative purpose of BIPA.

The Illinois Supreme Court looked at legislative history for indications of the evil BIPA was intended to remedy.[91] By considering the Pay By Touch bankruptcy which led to BIPA's enactment, the court concluded that the Illinois Legislature saw violations of BIPA as a "real and significant" harm worthy of a remedy.[92] BIPA was meant to prevent biometric information security breaches before they happened. The act did this by: (1) "imposing safeguards," and (2) providing "substantial potential liability" for violations.[93] To meet BIPA standards, third-party companies needed only to provide information to users about why and for how long their biometric identifier or biometric information was being stored and obtain their consent; there were no requirements or standards regarding further protections

---

[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] *See id.*
[89] *Id.* ¶ 34.
[90] *Id.* (quoting Rosenbach v. Six Flags Ent., 2017 IL App (2d) 170317, ¶ 23, *rev'd*, 2019 IL 123186).
[91] *See id.* ¶ 35.
[92] *Id.* ¶¶ 34–35.
[93] *Id.* ¶ 36.

of biometric information.[94] Due to the ease of compliance and important goals associated with BIPA, the *Rosenbach* court thought it more likely that the Legislature wanted violations to lead to a cause of action.[95]

Along with simple guidelines, effective enforcement required plaintiffs to have standing for pure violations. Since BIPA did not allow the Attorney General to bring suit, BIPA could not be enforced without a private right of action for violations.[96] There were "no other enforcement mechanism[s] . . . available."[97] Requiring plaintiffs to prove actual injury would mean that almost all suits brought by private individuals would fail for lack of standing.[98] BIPA only imposed a strong incentive to conform to the simple guidelines if private rights of action were allowed for violations of the law.[99] If the court had ruled against Rosenbach, there would have been no consequences for BIPA violations, and BIPA would have had no practical effect.[100]

3. Issues Not Addressed by the *Rosenbach* Decision

While the *Rosenbach* case was decided correctly, it did not address the changing technological environment. With the exponential growth of technological innovations and the dominance of devices in daily life, BIPA must be read broadly to, at the minimum, provide a basis for future protections. Five areas were left undeveloped after the *Rosenbach* decision: (1) the nature of the created rights, (2) enforcement and the remedial gap, (3) financial limitations, (4) minors' rights, and (5) gaps in notice.

a. The Nature of the Rights Created by BIPA

The *Rosenbach* decision did not specify what kind of rights BIPA created.[101] Logically, the right to know how one's biometric information is used stems from a type of property right. Personal information belongs to the individual from whom it was collected,

---

[94] 740 ILL. COMP. STAT. ANN. 14/15(b)(1)–(b)(3) (West 2010).

[95] *Rosenbach*, 2019 IL 123186, ¶ 37.

[96] Natalie Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020*, MINTZ, (Jan. 15, 2020), https://www.mintz.com/insights-center/viewpoints/2826/2020-01-15-anatomy-biometric-laws-what-us-companies-need-know-2020 [https://perma.cc/7TP5-MYNC]; *Rosenbach*, 2019 IL 123186, ¶ 25.

[97] *Id.* ¶ 37.

[98] *Id.* ¶ 12.

[99] *See id.* ¶ 25.

[100] *See id.*

[101] *See id.*

and that individual should have a say in how it is stored and used by third parties. The requirement of notice and implied consent can be seen as a license, which individuals grant to the third parties to use their personal information in a specified way. By identifying BIPA rights as property rights, the court could have set the stage to extend common law presumptions about property to personal information, facilitating BIPA's application to newly advancing technologies and services.

b. Enforcement and the Remedial Gap

BIPA's purpose is to discourage indiscriminate use and exploitation of personal biometric information, with hefty fines for each violation.[102] *Rosenbach* was a turning point in BIPA enforcement, but the decision simply allows individuals suffering from a BIPA violation their day in court.[103] As of yet, there is no assurance that violations will be punished.[104] There has not yet been a substantial plaintiff victory to encourage other plaintiffs to shoulder the time and expense of pursuing such claims, although several BIPA cases are underway after the *Rosenbach* decision.[105]

If a substantial plaintiff victory occurs, the next challenge for the court would be to make the plaintiff whole. BIPA, as well as other state laws inspired by it, does not outline a method to estimate and remedy the damage caused by a violation.[106] Even if a BIPA violation is punished, individuals do not have control over where their biometric information is stored or what will become of it in the future.[107] Even if the violating company were to pay monetary damages for its violation, there is no indication what the next step would be to protect the biometric information.

Money is not necessarily the only remedy. Courts could enjoin companies to delete the information collected in violation of

---

[102] 740 ILL. COMP. STAT. ANN. 14/20 (West 2010).

[103] *Rosenbach*, 2019 IL 123186, ¶ 38.

[104] *See* Douglas A. Darch & Jenna Neumann, *BIPA After Rosenbach—A Broad Interpretation by Illinois Courts*, EMP. REP. (May 28, 2019), https://www.theemployerreport.com/2019/05/bipa-after-rosenbach-a-broad-interpretation-by-illinois-courts [https://perma.cc/AM83-C79V].

[105] *Id.*

[106] *See* 740 ILL. COMP. STAT. ANN. 14/20; Lori Tripoli, *Resurgent BIPA More Than Second Fiddle to CCPA?*, COMPLIANCE WK. (Feb. 21, 2020, 11:36 AM), https://www.complianceweek.com/data-privacy/resurgent-bipa-more-than-second-fiddle-to-ccpa/28481.article [https://perma.cc/U84C-7MSD]; TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2017); WASH. REV. CODE ANN. § 19.375.020(1) (West 2017).

[107] *See* 740 ILL. COMP. STAT. ANN. 14/15.

BIPA. Although these considerations affect the way in which BIPA should be read, the *Rosenbach* court punted this issue.[108]

c. Financial Limitations

While BIPA's goal is admirable, its provisions do not ensure equal rights over personal information.[109] The sale of personal information draws huge profits that allow larger companies to reduce the cost of their services. Given the prevalent and constantly evolving use of technology in the modern world, the idea of not agreeing to company policies is almost unthinkable; ninety-one percent of Americans, for example, agree to "legal terms and services conditions without reading them."[110] If an individual opts not to agree to the biometric collection terms, her only current options are not to use that technological service or to find an alternative, which would likely be more expensive. Larger companies often have territorial dominance, particularly in rural areas; often, choosing not to agree to a company's terms means, at worst, being excluded from basic services.[111] Lower-income individuals in areas of economic distress may not have the luxury of choosing a more expensive service that does not require consumers to opt in to biometric information collection.[112]

Additionally, if the entire nationwide market has similar collection policies—a likely scenario when data collection is so lucrative—then the choice not to agree to data collection in fact requires the decision not to engage in certain technological uses altogether.

d. Minors' Rights

In the modern world, minors have more social media accounts and devices than ever before.[113] Ninety-five percent of teens use smartphones, and forty-five percent spend most of their

---

[108] *See Rosenbach*, 2019 IL 123186.

[109] *See* 740 ILL. COMP. STAT. ANN. 14/15.

[110] Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017, 7:30 AM), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [https://perma.cc/EZ3X-BJW8].

[111] *See* Sam Fleming, *Decline of Rural U.S. Businesses Contrasts with Prospering Cities*, FIN. TIMES (Oct. 15, 2018), https://www.ft.com/content/fa3419a2-d019-11e8-a9f2-7574db66bcd5 (subscription required).

[112] *See id.*

[113] Monica Anderson & Jingjing Jiang, *Teens, Social Media & Technology 2018*, PEW RSCH. CTR. (May 31, 2018), https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/ [https://perma.cc/P8LK-VB86].

day online.[114] With this privilege comes many dangers. The law generally presumes that minors are less able to recognize such dangers and concerns than adults, leading to more paternal protections for minors.[115] Given the quick rise of technologies that use biometric information, minors have been well-educated on the dangers of sharing information with strangers online; however, they are less informed and less concerned about the long-term consequences of personal data breaches.[116]

BIPA does not require additional consent from parents or guardians before the personal data of minors is collected. The *Rosenbach* decision briefly mentioned the issue of Alexander's minority,[117] but did not address concerns stemming from it; while the court could not judicially create new provisions of BIPA, explicit references to minors' rights or a statement of concern focused at the legislature could have provoked an update or revision of an important aspect of BIPA rights. The federal Family Educational Rights and Privacy Act ("FEPA"), for example, allows parents to "opt out of the disclosure of directory information" with third parties.[118] Educational information changes every few years, whereas biometric information is forever.[119] Children do not grow out of their collected biometric information in the same way that they outgrow their school systems.[120] Protections similar to FEPA should apply to information that has more substantial long-lasting implications regarding a minor's privacy.

II. CCPA'S BIOMETRIC INFORMATION PROTECTIONS

CCPA focuses on biometric information collected for commercial purposes.[121] Biometric information is covered under CCPA's broader definition of personal information used "to build a profile about a consumer," which is covered under "[b]usiness pur-

---

[114] *Id.*

[115] *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 2020), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 [https://perma.cc/F72K-A26K].

[116] Anne Collier, *Internet Safety: Teenagers Are Well Aware of Dangers Online*, CHRISTIAN SCI. MONITOR (June 18, 2012), https://www.csmonitor.com/The-Culture/Family/Modern-Parenthood/2012/0618/Internet-safety-Teenagers-are-well-aware-of-dangers-online [https://perma.cc/4RZS-NZJ6].

[117] Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶ 8.

[118] 34 C.F.R. § 99.37(b) (2020).

[119] *See Rosenbach*, 2019 IL 123186, ¶ 35 (citation omitted).

[120] *See id.*

[121] CAL. CIV. CODE § 1798.140(o)(1)(E) (West 2020).

pose."[122] Biometric information that is not collected "in the ordinary course of business" is not covered by CCPA.[123]

Under CCPA, consumers must receive notice of any changes to company policy within the past twelve months.[124] Companies must provide consumers with "clear and conspicuous" methods of contacting companies to request that they not sell the individual's data.[125] This strict formality is loosened for opt-outs; an authorized third person can opt out on the consumer's behalf.[126]

Companies are responsible not only for the biometric information they store, but also for any such information that they disseminate to other companies.[127] Upon a deletion request, the company must delete the personal information and "direct any service providers to delete" the information.[128] CCPA, therefore, impliedly requires companies to track whom they give personal information to, and provide third parties with notice when the consumer changes any authorization, unless an exception applies.[129]

The preamble of CCPA eliminates the standing problem addressed in *Rosenbach* by creating causes of action for violations.[130] Whereas BIPA cases have only recently started multiplying since the *Rosenbach* decision,[131] CCPA will hopefully bypass the slow growth of private suits by explicitly granting standing based on certain types of violations. The Attorney General may bring suit if companies have not cured violations within 30 days, but an individual may bring suit only for violations "in connection with certain unauthorized access and exfiltration, theft, or disclosure of . . . nonencrypted or nonredacted personal information."[132] Penalties mimic the high rates from BIPA.[133]

---

[122] *Id.* § 1798.140(d)(4).

[123] *Id.* § 1798.110(d)(2). Personal information is information "reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." *Id.* § 1798.140(o)(1). Biometric information covers "an individual's physiological, biological, or behavioral characteristics . . . that can be used . . . to establish individual identity." *Id.* § 1798.140(b).

[124] *Id.* § 1798.130(a)(5).

[125] *Id.* § 1798.135(a)(1). "[A]t a minimum," companies must have a toll-free number and a website address in which individuals can request information. *See id.*; *see also id.* § 1798.130(a)(1).

[126] *Id.* § 1798.135(c).

[127] *Id.* § 1798.105(c).

[128] *Id.*

[129] *See id.*

[130] S.B. 1121, 2018 Leg., Reg. Sess. (Cal. 2018).

[131] Maatman et al., *supra* note 39.

[132] Cal. S.B. 1121.

Businesses cannot discriminate against consumers who exercise their CCPA rights, but they may "[c]harg[e] different prices or rates" and may "[p]rovid[e] a different level or quality of goods or services" as long as "that difference is reasonably related to the value provided . . . by the consumer's data."[134] Companies can offer financial incentives to encourage individuals to agree to biometric information collection, as long as the terms are clear.[135]

CCPA does not stop companies from collecting biometric information from minors younger than sixteen; rather, it only stops them from selling it without a parent or guardian's affirmative authorization.[136] Actual knowledge of a consumer's age is imputed, so companies cannot use willful blindness as a defense.[137]

If a consumer opts out, the company must wait at least a year before asking for authorization for the sale of the personal information again.[138] A company is only obligated to comply with a request from an individual for the current status of the company's policy on collected data twice a year.[139] To further protect the biometric information, businesses must take reasonable steps to determine whether the request is a "verifiable consumer request."[140]

Although 500,000 businesses in the United States are affected by CCPA, a 2019 survey said "only 8% of businesses [were] prepared" for its enactment.[141] CCPA does not specify enforcement.[142] Companies were, therefore, waiting to see how it would be enforced before weighing "the cost of compliance against the risk and cost of being fined."[143]

A survey found that most businesses were "aware (20%) or [were] educating themselves (58%) about CCPA," while "22% did

---

[133] *Id.*

[134] § 1798.125(a)(1)(B)–(C), (a)(2).

[135] *Id.* § 1798.125(b)(1)–(3). "[M]aterial terms" of such programs must be clearly described to the consumer for the opt-in authorization to be valid; such consent can be revoked at any time. *Id.* § 1798.125(b)(3).

[136] *Id.* § 1798.120(c). Authorization may be given after collection. *Id.* § 1798.120(d).

[137] *Id.* § 1798.120(c).

[138] *Id.* § 1798.135(a)(5).

[139] *Id.* § 1798.130(a)(7)(b). Requested information must be sent to the consumer within 45 days. *Id.* § 1798.130(a)(2).

[140] *Id.* § 1798.130(a)(2).

[141] Haggin, *supra* note 32; April Berthene, *Majority of Businesses Are Unprepared for California Privacy Act*, DIGIT. COM. 360 (Aug. 26, 2019), https://www.digitalcommerce360.com/2019/08/26/majority-of-businesses-are-unprepared-for-california-privacy-act/ [https://perma.cc/8UCG-3J3R].

[142] Berthene, *supra* note 141.

[143] *Id.*

not know about it."[144] Another report estimates that the cost of initial compliance may reach $55 billion.[145] These costs may have been exaggerated since many California businesses recently had to comply with Europe's General Data Protection Regulation ("GDPR").[146] Nonetheless, many companies were "scrambling to build [the] tools" to comply with the CCPA.[147] They saw expensive compliance as a long-term business decision.[148] Smaller firms were expected to be disproportionately affected by CCPA, just as with the GDPR.[149]

III. GAPS BETWEEN BIPA AND CCPA

This Part will compare BIPA and CCPA to show how the two overlap regarding the questions left unanswered in *Rosenbach*. CCPA expands on, but does not fully cover, the gaps remaining after the *Rosenbach* decision: (1) the nature of the created rights, (2) the remedial gap, (3) financial limitations, (4) minors' rights, and (5) gaps in notice.

A. The Nature of the Created Rights

Neither BIPA nor CCPA specifically addresses the nature of the created rights.[150] Without a clear indication of the type of right, future courts will struggle with how to promote BIPA's and CCPA's goals. Given the context in which both laws were enacted, the laws filled the void of consumer vulnerability to ensure sufficient protections in the future.[151] If these rights were specified as property rights, future courts could apply existing common law to evolving and unanticipated situations.

While courts have traditionally been reluctant to expand property rights to human bodies, they should not have the same hesitation about applying these rights to biometric information. In the modern world, biometric information is an alienable resource that individuals can use to facilitate their lives.[152]

---

[144] *Id.*

[145] Feiner, *supra* note 37.

[146] *Id.*

[147] Haggin, *supra* note 32.

[148] Berthene, *supra* note 141.

[149] Feiner, *supra* note 37.

[150] *See* 740 ILL. COMP. STAT. ANN. 14/1–99 (West 2010); CAL. CIV. CODE § 1798.100–199.95 (West 2020).

[151] *See* 740 ILL. COMP. STAT. ANN. 14/5; *see also* H.B. 375, 2018 Gen. Assemb. (Cal. 2018).

[152] *See* Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶ 35.

CCPA expanded on BIPA's focus on the continued interest consumers have in their collected biometric information by requiring notice of updated company policy and allowing consumers to change their minds about how their biometric information is used.[153]

B. Enforcement and the Remedial Gap

Both BIPA and CCPA were enacted to prevent security breaches that compromise personal information, yet both disregard what happens to that information once compromised by failing to provide concrete methods to deal with such dangers.[154] CCPA's high penalties, like BIPA's, are meant to discourage negligent storage of personal information, not to compensate the individual for the breach.[155] Penalties will not restore control of someone's biometric information. In fact, CCPA specifies that any civil penalties recovered by the Attorney General will offset the cost of the trial.[156] Private enforcement is only available for a limited set of cases involving "unauthorized access and exfiltration, theft, or disclosure of a consumer's . . . personal information."[157] In an environment where defenses are reactive to breaches, such measures are unlikely to be particularly effective in promoting protection.[158]

Another concern is that CCPA does not seem to cover encoded or encrypted personal information.[159] Issues of pseudonymized, deidentified, and reidentified information are only addressed relating to research.[160] Only "nonencrypted and nonredacted personal information" is protected from "unauthorized access and exfiltration, theft, or disclosure" resulting from the business' violation of the duty of care.[161] This difference creates a distinction that would not be otherwise inferred and exhibits the legislature's assumption that encrypted information is safe from

---

[153] § 1798.135(a)(4)–(6), (c).

[154] *See* 740 ILL. COMP. STAT. ANN. 14/5; *see also* Cal. H.B. 375.

[155] § 1798.155(b).

[156] *Id.* § 1798.155(c).

[157] Cal. H.B. 375.

[158] *See* KPMG, *Moving from Reactive Cyber Security to Proactive Cyber Security: Six Steps to Achieving Prosilience*, FED. NEWS NETWORK (July 29, 2019, 11:47 AM), https://federalnewsnetwork.com/kpmg/2019/07/moving-from-reactive-cyber-security-to-proactive-cyber-security-six-steps-to-achieving-prosilience/ [https://perma.cc/JL4W-7V6Q].

[159] § 1798.140(s)(2)–(6).

[160] *Id.* § 1798.140(s)(2), (7).

[161] *Id.* § 1798.150(a)(1).

abuse or misuse.[162] BIPA also underestimated the capabilities of hackers and modern computers.[163] Information encrypted or protected under current industry standards is not safe from hackers, who do not need to compromise the encryption formula in order to gain access to encrypted information.[164] Instead, they can simply compromise computers containing the encryption "key," allowing them to decrypt any information protected by that encryption.[165]

Additionally, there may be a disconnect between protective schemes, like BIPA's private enforcement and CCPA's mixed private-and-public enforcement scheme. While CCPA protections will apply to Illinois citizens if companies choose uniform nationwide application, Illinois state courts will limit suits to BIPA violations.[166]

C. Financial Limitations

Unlike BIPA, CCPA addresses concerns of financial pressure by prohibiting service discrimination based on opting out of a company's personal information collection policies.[167] CCPA attempted to cover this gap by prohibiting businesses from discriminating against consumers who opted-out of the data collection policy.[168] While this appears to create alternatives, other CCPA provisions could be read to negate this important prohibition.[169] The following section states that businesses may charge consumers different prices or rates "if that difference is reasonably related to the value provided to the consumer by the consumer's data."[170] As previously stated, the sale of private information provides huge value for companies. While it is reasonable to

---

[162] *See id.*

[163] *See* Jon Porter, *Huge Security Flaw Exposes Biometric Data of More Than a Million Users*, THE VERGE (Aug. 14, 2019, 6:58 AM), https://www.theverge.com/2019/8/14/20805194/suprema-biostar-2-security-system-hack-breach-biometric-info-personal-data [https://perma.cc/8J45-7RD5]. BIPA does not require any higher standard of protection for collected biometric information than that required for other confidential and sensitive information. *See* 740 ILL. COMP. STAT. ANN. 14/15 (West 2010).

[164] *See* Porter, *supra* note 163.

[165] Yaron Guez, *6 Encryption Mistakes That Lead to Data Breaches,* CRYPTERON, https://www.crypteron.com/blog/the-real-problem-with-encryption/ [https://perma.cc/Z3TQ-K2W4] (last visited Mar. 21, 2021).

[166] *See* 740 ILL. COMP. STAT. ANN. 14/20.

[167] *See* § 1798.125(a).

[168] *See id.* § 1798.125(a)(1).

[169] *See id.* § 1798.125(a)(2).

[170] *Id.*

allow companies to charge more when they make less profit on a consumer's use of their service, the lack of a measurable standard negates the purpose of an alternative. If consumers opt out of the collection policy, their use of the service will be different from consumers who opt in, as they will not have access to the same features and will be charged more to compensate the company for the lack of external profit from the sale of their personal information. Two of the requirements for nondiscrimination will therefore necessarily be broken by this different treatment: not charging different rates and not providing different levels of service.[171] CPPA has not provided a measurable standard to evaluate the reasonability of alternative services.[172]

BIPA did not address the necessity of alternatives, but CCPA has not succeeded in plugging the gap.[173] There is still room for discrimination, which will likely mean that lower income individuals will be incentivized to surrender their privacy rights.

D. Minors' Rights

Given the prevalence of technology in daily life, minors are more vulnerable than ever when their personal information is surrendered to a company for reasons that they do not fully understand.[174] Most minors do not think about cybersecurity or privacy when they use new technologies;[175] rather, they are concerned about following popular trends without awareness or consideration of the long-term ramifications of their choices.[176]

While CCPA—unlike BIPA—addresses minors' rights, it fails to address what notice or authorization is required of the minor once he or she reaches maturity.[177] Presumably, the individual on file will be the parent or guardian. Together with

---

[171] *See id.* § 1798.125(a)(1)(B)–(C).

[172] *See id.* § 1798.125.

[173] *See id.* § 1798.125(a).

[174] *See Kids and Computer Security*, FED. TRADE COMM'N (Sept. 2011), https://www.consumer.ftc.gov/articles/0017-kids-and-computer-security [https://perma.cc/MM9R-U65G].

[175] Renee Morad, *Why Teens Are at Risk for Identity Theft*, NORTON LIFELOCK (July 21, 2014), https://www.lifelock.com/learn-identity-theft-resources-teens-risk-identity-theft.html [https://perma.cc/3T2P-LT48].

[176] Michael Cañares, *Teenage Clicks: Can Teens Protect Their Privacy on Social Media?*, WORLD WIDE WEB FOUND. (Sept. 4, 2018), https://webfoundation.org/2018/09/teenage-clicks-can-teens-protect-their-privacy-on-social-media/ [https://perma.cc/5LDZ-6F76].

[177] *See* § 1798.120(c).

BIPA's failure to mention minors' rights, this leaves a significant gap in the protection of the personal information of minors.[178]

E. Gaps in Notice

While the overall idea of notice in CCPA is good, it creates a loophole period during which companies could sell personal information before individuals are made aware of any policy changes.[179] If a consumer checked the policy before the change, they would not know to use their full rights under CCPA until it was too late to prevent the sale. Companies could foreseeably deprive a consumer of any cause of action through such a technicality. BIPA would not cover this behavior either; it only requires notice of the policy at the time the company collects the personal information.[180]

IV. RECOMMENDATIONS TO FILL GAPS BETWEEN BIPA AND CCPA

CCPA does not fully close the gaps in BIPA left by the *Rosenbach* decision. CCPA's language was broadened slightly by Assembly Bill 713 in September 2020,[181] but even further specification beyond the current proposal would help both courts and consumers. Although CCPA and BIPA in conjunction provide citizens with expanded protections in the technological era, important issues remain unanswered.

Increased data protection has become particularly important as data privacy issues have begun to damage American business practices abroad. The European Union's top court recently ruled that European data was not adequately protected from government surveillance in the United States.[182] In comparison with Europe's GDPR, American data privacy laws remain scattered

---

[178] *See* 740 ILL. COMP. STAT. ANN. 14/15 (West 2010).

[179] *See* § 1798.130(a)(7), (b).

[180] 740 ILL. COMP. STAT. ANN. 14/15(b).

[181] *CCPA Amendment Update: California Governor Approves CCPA Amendment with Exceptions for HIPAA De-Identified Information and Other Health Data*, NAT'L L. REV. (Oct. 9, 2020), https://www.natlawreview.com/article/ccpa-amendment-update-california-governor-approves-ccpa-amendment-exceptions-hipaa [https://perma.cc/26LZ-WJRZ]; A.B. 713, 2020 Gen. Assemb. (Cal. 2020).

[182] Michael Birnbaum, *Top E.U. Court Ruling Throws Transatlantic Digital Commerce into Disarray over Privacy Concerns*, WASH. POST (July 16, 2020, 10:33 AM), https://www.washingtonpost.com/world/europe/top-eu-court-ruling-throws-transatlantic-digital-commerce-into-disarray-over-privacy-concerns/2020/07/16/d2c0fe06-c736-11ea-a825-8722004e4150_story.html [https://perma.cc/XE2F-87L2].

and rare. The previous data protection compromise between American and European companies, called the "Privacy Shield," was found to be too lax for the EU's more exacting data protection standards.[183]

The COVID-19 pandemic has also brought the gap in personal information data security to the forefront of politics. As employers struggle to screen employees per state and federal health and workplace regulations, local governments are rushing to provide data protection for any personal, medical, or contact-tracing data collected. Data collection is also starting to be seen as a new frontier to raise public funds; in New York, a bill was recently proposed that would tax data collection to cover COVID-19 expenses.[184] The pandemic has reignited hopes for a federal data protection bill called the COVID Consumer Data Protection Act, which was proposed in May 2020 and continues to languish before the Committee on Commerce, Science, and Transportation.[185]

States like Illinois should pass language similar to CCPA to provide their citizens with causes of action for the *de facto* nationwide protections of CCPA. Hopefully, states can use California as a model to update their own laws and to continue improving on CCPA's provisions.

Specifically identifying the nature of the created rights will strengthen BIPA's and CCPA's protective purposes. Given individuals' continued interests in their immutable biometric information, courts could interpret consent to collect, store, or use biometric information as a kind of lease. Both parties benefit from the collection; companies receive financial benefit, while consumers receive more secure and efficient service. Specific labeling of the collection, storage, and use of biometric information as a lease would allow courts to adapt these statutes to evolving technologies through analogy to existing common law

---

[183] *Id.*

[184] *New Taxes on the Digital Economy: A Closer Look at the New York Data Tax Proposal*, JDSUPRA (Mar. 25, 2021), https://www.jdsupra.com/legalnews/new-taxes-on-the-digital-economy-a-6954569/ [https://perma.cc/D749-88EV]; Eric Adams & Andrew Gounardes*, A Tax on Data Could Fix New York's Budget*, WALL ST. J. (June 1, 2020, 7:12 PM), https://www.wsj.com/articles/a-tax-on-data-could-fix-new-yorks-budget-11591053159 [https://perma.cc/7ZP7-QX9H].

[185] Junaid Odubeko & Andrew Tuggle, *Federal Privacy Bill To Focus on COVID-19*, BRADLEY (May 5, 2020), https://www.bradley.com/insights/publications/2020/05/federal-privacy-bill-to-focus-on-covid19 [https://perma.cc/2YVT-PX65]. The bill was referred to the Committee on Commerce, Science, and Transportation. COVID-19 Consumer Data Protection Act of 2020, S. 3663, 116th Cong. (2020).

and case law concerning leases. Not only would this label make interpretation simpler for courts, but it would also emphasize that the collected information still fundamentally belongs to the individual rather than the company. It would eradicate the possibility that sensitive biometric information could be sold as assets of a bankrupt company.

If biometric information storage were subject to a lease, the gap in notice would be simpler to fill. The more specific forms and terms used in lease agreements could be mimicked in collection notices. By requiring additional language before companies shared biometric information, legislatures could preempt market transformation rather than constantly reacting with legislation when new problems arise in the evolving technology market. Consumers would then have notice when their biometric information is passed to other entities, regardless of prior consent to the original collector, and would remain aware of who possessed their biometric information. Consumers would have more power to enforce the protection of their sensitive, immutable information.

To ensure compliance, BIPA and CCPA must broaden private enforcement actions or expand current departmental purposes to monitor biometric information collection. CCPA encourages limited forms of private enforcement that will curb particularly egregious behavior; other violations remain at the Attorney General's discretion.[186] Collection of penalties incentivizes the Attorney General to pursue such cases, but each undertaking would still cost substantial amounts of money and time.[187] Most likely, the Attorney General will pursue larger companies, whose violations would produce higher penalties; violations by smaller companies, while no less damaging for individual consumers than larger violations, could escape prosecution. The low percentage of companies preparing to comply illustrates that many are waiting to see how strict enforcement will be before complying.

New technologies could eventually be used to fill these gaps. The advent of quantum computers provides a tantalizing option; a sophisticated, rare, and expensive new technology could reduce

---

[186] *See* CAL. CIV. CODE § 1798.155(b) (West 2020).

[187] *See id.* § 1798.155(c).

the threat of hacks, but it will be years before such technology becomes effective.[188]

Until then, statutory protections must be updated to protect biometric information vulnerable to hackers who seize encryption keys.[189] BIPA and CCPA should be amended to encourage companies to use protective measures beyond what is required for less sensitive information. Protective requirements should be expanded to cover computers and devices that encrypt and decrypt biometric information, or the legislatures should pass separate, broader data privacy restrictions upon which BIPA and CCPA can rely.

Legislatures should also set a measurable standard for acceptable alternatives for individuals who opt out of such collection. The biometric information market from each previous year could provide a measurable standard to determine the financial benefit such information provides. Without standards, courts cannot ensure that alternatives to opting in are not false choices that incentivize lower-income individuals to surrender their biometric information privacy rights for financial reasons.

Legislatures should also ensure that, upon maturity, minors receive full information about how their guardians disseminated their biometric information. Companies storing a former minor's biometric information should be required to contact either the individual or her guardian to inform her, or them, of policies and receive updated consent. Otherwise, if a minor's legal guardian can decide on the use of the minor's biometric information, the minor may not know or remember who holds her biometric information or how it is stored and protected.

If these recommendations had been in place in 2014, Six Flags' website would have informed Stacey Rosenbach about how Alexander's biometric information would be collected for the season pass. Mrs. Rosenbach could have chosen to buy Alexander a one-time ticket instead. At Six Flags, Alexander would not have been able to surrender his biometric information without notice to Mrs. Rosenbach about why and how the information would be used. Alexander's biometric information could not have been collected without Mrs. Rosenbach's consent.

---

[188] Adrian Cho, *Cryptographers Scramble To Protect the Internet from Attacks Armed with Quantum Computers*, SCI. MAG. (Aug. 21, 2019, 1:15 PM), https://www.sciencemag.org/news/2019/08/cryptographers-scramble-protect-internet-hackers-quantum-computers [https://perma.cc/S3WE-WVMU].

[189] *See id.*

If Six Flags chose to sell or share Alexander's biometric information with other companies, Mrs. Rosenbach would be updated and allowed to opt out of new uses not previously disclosed. She would have been given an option to continue comparable services measured relative to the interrupted financial benefit Six Flags failed to acquire from Alexander's biometric information. If evolving technology or increasingly sophisticated hacks worried the Rosenbachs, they could have contacted Six Flags to have the information deleted. If over the years Alexander or Mrs. Rosenbach forgot about Alexander's thumb scan, Six Flags would still have contacted Alexander upon maturity and asked for updated consent. Alexander could then have chosen whether or not he wanted Six Flags to retain his biometric information. With these recommendations in place, the Rosenbachs would have a substantially more central role in the protection of Alexander's biometric information; they would not have been left wondering what was happening to Alexander's immutable biometric information and who had access to it.