Maine Law Review

Volume 75 | Number 1 Article 7

March 2023

Your Biometric Data is Concrete, Your Injury is Imminent and Particularized: Articulating a BIPA Claim to Survive Article III Standing After TransUnion v. Ramirez

Kelsey L. Kenny
University of Maine School of Law, kelsey.kenny@maine.edu

Your Biometric Data is Concrete, Your Injury is Imminent and Particularized: Articulating a BIPA Claim to Survive Article III Standing After TransUnion v. Ramirez

Cover Page Footnote

CIPP/US; J.D. Candidate, University of Maine School of Law Class of 2023. I am grateful to Professor Scott Bloomberg for his support, guidance, and insight through this process; to the Maine Law Review team for their time and attention; and to my dear family and friends who believed in me through it all. To the Supreme Court, a question: If a tree falls in the forest and no Justice is around to hear it, does it still make a sound? All errors are my own.

YOUR BIOMETRIC DATA IS CONCRETE, YOUR INJURY IS IMMINENT AND PARTICULARIZED: ARTICULATING A BIPA CLAIM TO SURVIVE ARTICLE III STANDING AFTER *TRANSUNION V. RAMIREZ*

Kelsey L. Kenny

YOUR BIOMETRIC DATA IS CONCRETE, YOUR INJURY IS IMMINENT AND PARTICULARIZED: ARTICULATING A BIPA CLAIM TO SURVIVE ARTICLE III STANDING AFTER *TRANSUNION V. RAMIREZ*

Kelsey L. Kenny*

ABSTRACT

Biometric data is a digital translation of self which endures in its accuracy for one's entire lifespan. As integral elements of modern life continue to transition their operations exclusively online, the verifiable "digital self" has become indispensable. The immutable and sensitive nature of biometric data makes it peculiarly vulnerable to misappropriation and abuse. Yet the most frightening is the unknown. For an individual who has had their digital extension-of-self covertly stolen or leaked, the dangers that lie in the technology of the future are innumerable.

The Illinois legislature recognized the danger associated with the cavalier collection and handling of biometric data in 2008, passing the Biometric Information Privacy Act (BIPA) to facilitate a higher standard for consumer protection. BIPA's key feature is a private right of action awarding not less than $1,000 for each instance of non-compliance with certain enumerated data collection and handling procedures. In the years since its enactment, classes of Illinois plaintiffs have successfully won multimillion-dollar judgments in state court. However, when an out-of-state defendant removes to federal court, Article III standing often proves to be an insurmountable threshold for the plaintiff class. This issue delays the plaintiff class's relief and undermines the goal of the Illinois legislature.

This Comment summarizes the state of legal protection of biometric data in the United States. It then explains the development of Article III standing doctrine as it pertains to statutorily prescribed privacy harms. Next, this Comment reviews Article III standing in the context of BIPA litigation specifically. Finally, it recommends an articulation of the injury at the heart of BIPA likely to confer Article III standing to assist plaintiff's counsel in evading the quagmire. It is a call to attention and a call to arms; biometric data handling requires the same care as the handling of the physical body.

* CIPP/US; J.D. Candidate, University of Maine School of Law Class of 2023. I am grateful to Professor Scott Bloomberg for his support, guidance, and insight through this process; to the Maine Law Review team for their time and attention; and to my dear family and friends who believed in me through it all. To the Supreme Court, a question: If a tree falls in the forest and no Justice is around to hear it, does it still make a sound? All errors are my own.

INTRODUCTION

Maybe you own a smart phone or know someone who does. If you do, you are likely familiar with the process of placing your thumb on the "home" button or briefly peering into the built-in camera so that your device scans your anatomy, verifies your identity, and unlocks. The identity-verification mechanism built into many smartphones is one small example of how advancements in computer science, biometric data-gathering hardware, and artificial intelligence (AI) have come to proliferate in our daily lives.[1] Although the ways in which we engage with technology may often seem obvious, devices with the capacity to discretely collect and contribute data to the "Internet of Things"[2] have grown increasingly commonplace and actively undermine our awareness of the extent to which we are enmeshed in the "ecosystem of ubiquitous computing."[3] Not all ecosystems of data processing are innocuous, nor should they operate without stringent regulatory supervision. In particular, the prevalence of biometric data processing[4] should not "mask the danger that it poses."[5]

The commercial use of biometric data is far more dangerous to the consumer than most other types of sensitive data processing for three main reasons.[6] First, "[t]he immutable nature" of biometric data means that once this data has been compromised, the individual is exposed to heightened risk of "theft, misuse, and misappropriation" for the rest of their life with practically no legal recourse.[7] Second, "[t]he richness of information extractable from biometric data makes drifts in scope, nature, and purpose extremely common" and nearly unlimited.[8] Finally, "[t]he conspicuous nature of many biometrically scannable identifiers" like one's face, voice, or gait "makes such data potentially very public, and has already led to a significant breach of privacy whenever people are in public places, physically or virtually."[9]

---

1. *See* LYDIA KOSTOPOULOS, DECOUPLING HUMAN CHARACTERISTICS FROM ALGORITHMIC CAPABILITIES 3 (2021).

2. Often referenced as "IoT," this phrase describes the network of household objects that have discrete embedded sensors installed to collect, process, store, and share data with the internet. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD 5 (2015).

3. *Id.* "The sheer volume of data that even a small number of devices can generate is stunning"; an IoT product will generate, on average, one new data point approximately every six seconds. *Id.* at 14.

4. The "unlock" mechanism in Apple's iPhone is an example. *Face ID & Privacy*, APPLE, https://www.apple.com/legal/privacy/data/en/face-id/ [https://perma.cc/T5BD-824T].

5. RYAN CARRIER ET AL., BIOMETRIC DATA: HUMANITY'S MOST PRECIOUS DATA 2 (2022). Several international human rights advocacy groups have come together to call for a blanket ban on the use of biometric recognition technologies in public spaces due to the sensitive nature of the data. *See* AccessNow et al., *Open Letter Calling for a Global Ban on Biometric Recognition Technologies that Enable Mass and Discriminatory Surveillance* (June 7, 2021), https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf. They argue, "[n]o technical or legal safeguards could ever fully eliminate the threat [this technology] pose[s]." *Id.* at 1.

6. CARRIER ET AL., *supra* note 5, at 3.

7. *Id.*; *see also* 740 ILL. COMP. STAT. 14/5(c) (2022).

8. CARRIER ET AL., *supra* note 5, at 3. "Drift" in this context means that the company collecting the data for one purpose may use it for another purpose without discretion. *See id.*

9. *Id.* Suddenly, CCTV video surveillance or Zoom conference recordings present new opportunities for biometric data breach and novel forms of abuse.

Although the heightened sensitivity of biometric data in the private commercial context has not gone entirely unrecognized by regulatory authorities in the United States,[10] the conspicuous lack of consensus as to how to best address this problem undermines the work of the more proactive state regimes that have been quicker to recognize the gravity of the situation. Illinois is a pioneer in this field. It enacted the country's first biometric information privacy statute in 2008 known as the Biometric Information Privacy Act (BIPA).[11] BIPA is unique because it is the earliest state regulation of biometric information in the private commercial context. More importantly, it creates a private right of action for Illinois residents to recover liquidated damages without the need for the plaintiff to show additional injury when a company fails to comply with the statutorily prescribed data handling practices.[12] Over the course of the last few years, classes of Illinois "plaintiffs have sued more than [two hundred] companies across a range of industries (from locker rental companies to tanning salons) for allegedly violating BIPA."[13] Even tech behemoths have not been exempt from massive settlements in BIPA actions.[14] Attorneys may now be particularly incentivized to bring class-actions under BIPA after the Ninth Circuit recently affirmed a district court decision awarding the class counsel's $97.5 million fee (15% of the total settlement against Facebook) despite arguments that the award was outrageous.[15] The consequences of BIPA's private right of action have had a meaningful effect on how even the nation's largest corporations shape their deployment of biometric data.[16] The potential for massive fines and creative arguments from plaintiffs' counsel, combined with the law's low injury threshold, effectively deters "companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses."[17] Attorneys general (the officials normally tasked with enforcing privacy regulations) are more predictable and susceptible to political pressure.[18] Actions brought by attorneys general even

10. *See infra* Section II.A.

11. *See generally* Biometric Information Privacy Act of 2008, Ill. Pub. Acts. 095-0994 (codified as 740 ILL. COMP. STAT. 14/5 (2022)).

12. *See* 740 ILL. COMP. STAT. 14/20 (2022).

13. Charles N. Insler, *How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act*, 43 S. ILL. U. L.J. 819, 819 (2019). BIPA is not a particularly new statute, yet its popularity among plaintiff class actions has been a relatively recent phenomenon. "In December 2015, the U.S. District Court for the Northern District of Illinois noted that it was 'unaware of any judicial interpretation of the statute.'" *Id.* (quoting Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015)).

14. *See, e.g.*, Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019). U.S. District Court Judge James Donato called the $650 million settlement in this case, one of the largest settlements ever for a privacy violation, a "landmark result." Jennifer Bryant, *Facebook's $650M BIPA Settlement 'a Make-or-Break Moment'*, IAPP (Mar. 5, 2021), https://iapp.org/news/a/facebooks-650m-bipa-settlement-a-make-or-break-moment/.

15. *In re* Facebook Biometric Information Privacy Litigation, No. 21-15553, 2022 WL 822923 (9th Cir. Mar. 17, 2022).

16. Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the U.S.?*, *in* REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS 96, 96–97 (Amba Kak ed., 2020) (detailing the requirements for deploying biometric technology in private enterprise generally).

17. *Id.* at 101.

18. *See id.*

facilitate the practice of making exemplary privacy compliance a soft marketing tactic for businesses.[19] For example, while Facebook's stock price rose notably after the FTC's historic five billion dollar fine was announced in the wake of the Cambridge Analytica privacy scandal, Clearview AI explicitly cited BIPA as the reason why it would no longer sell its services to private entities.[20] In this way, BIPA is one of the most effective privacy laws operating in the United States to date.

Yet BIPA is not perfect. "It has also forced judges to resolve longstanding issues of injury and standing for privacy violations" brought by plaintiffs in civil court.[21] Federal courts have thus been called upon to grapple with the strictures of Article III standing in the context of statute-created privacy harms. It is a thorny jurisprudence that has been significantly modified by the Supreme Court during the 2021 term to the detriment of plaintiff classes.[22] The Court in *TransUnion LLC v. Ramirez*, while addressing a class's standing under the private right of action for violation of certain provisions of the Fair Credit Reporting Act, "essentially nullified" the private right of action as an enforcement mechanism for privacy harms in federal court.[23]

A plaintiff class should not be deprived of their private right of action to vindicate a legally vested interest because of arbitrary procedural gatekeeping. Yet moving forward, BIPA plaintiffs will need to plead with exceptional dexterity to either avoid removal to federal court or somehow argue a form of injury that will survive Article III standing after *TransUnion*—a task so formidable that it is practically prohibitive.[24]

This past year, a student at St. Louis University School of Law reviewed the development of Article III standing jurisprudence under BIPA and asserted that if the Supreme Court were to settle the circuit split, they would likely side with the Seventh and Ninth Circuits, which have been amenable to conferring standing under BIPA's procedural provisions.[25] Perhaps unsurprisingly in the context of American privacy law, the legal atmosphere has materially shifted in the course of only a few months. With the Supreme Court's decision in *TransUnion*, this area of law is once again ripe for review.

The goal of this Comment is to articulate a model BIPA complaint that does not plead pecuniary injury, but that would still survive the test for Article III standing after *TransUnion.* In so doing, this Comment seeks to encourage the

19. *See, e.g.*, Ian Bogost, *Apple's Empty Grandstanding About Privacy*, THE ATLANTIC (Jan. 31, 2019), https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/ (explaining how Apple strategically claims to oppose the data economy in which it actively participates).

20. Hartzog, *supra* note 16, at 101.

21. *Id.* at 97.

22. *See, e.g.*, Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of* TransUnion LLC v. Ramirez, 101 B.U. L. REV. ONLINE 62, 62 (2021).

23. *Id.*; *see also* TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021).

24. *See generally* Solove & Citron, *supra* note 22, at 62–63 (Professors Solove and Citron believe that the modification of this threshold "is a profound usurpation of legislative power").

25. Michael McMahon, *Illinois Biometric Information Privacy Act Litigation in Federal Courts: Evaluating the Standing Doctrine in Privacy Contexts*, 65 ST. LOUIS U. L.J. 897, 932–33 (2021).

judicial development of critical statutory privacy protections for biometric data in America. To achieve this goal, this Comment describes and evaluates the circuit split presented in the Article III standing disputes that have risen out of BIPA litigation, particularly where no pecuniary injury is pled.

This Comment begins by briefly reviewing the current patchwork of U.S. federal and state law as it relates to the regulation of biometric information. Specifically, it argues that the legal infrastructure outside of Illinois fails to adequately protect consumer biometric data due to the absence of a private right of action for procedural violations. Next, this Comment describes the mechanics of BIPA and the contemporaneous federal litigation brought under the Act. This description focuses specifically on how the circuit courts have been divided on the issues of subject matter jurisdiction and Article III standing, as well as *TransUnion*'s holding and its deleterious implications for redressing privacy harms in federal court. Finally, this Comment concludes by proposing an articulation of the injury that the Illinois legislature sought to protect under BIPA that might successfully survive the current Article III standing analysis after *TransUnion*. This suggestion will aid practitioners as they engage in this critical litigation.

I. BACKGROUND

Biometric data, conceptually, can be broken down into two component parts. The first segment, "bio-," refers to biology (as in the scientific study of life and living organisms),[26] and "metric" refers to a rules-based system of measuring data quantitatively.[27] The combination of qualitative input (an aspect of one's physical anatomy, like facial structure) with numerical measurement values (for example, the proportionate distance between facial features), creates a map that is utterly unique to that particular individual.[28] As it is used today, biometric data may be broken down further into physiological and behavioral categories of information.[29] Physiological biometric data concerns features of the body, such as fingerprints, hand geometry, DNA, facial measurements, iris or retina color and shape, vein patterns, and blood type.[30] On the other hand, behavioral biometric data is derived from patterns of human behavior, like typing rhythm and key stroke dynamics, walking gait, voice and speech inflections, gestures, scrolling and swiping patterns, text recognition, geolocation and IP address, device use, and browser history.[31]

The most recognized modern use of biometric data technology is in the area of identity verification.[32] Often compared to a lock-and-key system, the pairing of

26. *See generally Biology*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/biology [https://perma.cc/R9BJ-8FH3].

27. *See generally Metric*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/metric [https://perma.cc/CHU2-N42A].

28. *See* Amba Kak, *Introduction*, *in* REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS 6, 6–8 (Amba Kak ed., 2020).

29. *See What Is Biometric Authentication?*, MITEK (July 11, 2019), https://www.miteksystems.com/blog/what-is-biometric-authentication.

30. *See id.*

31. *See id.*

32. *See* Donald L. Buresh, *Should Personal Information and Biometric Data Be Protected Under a Comprehensive Federal Privacy Statute That Uses the California Consumer Privacy Act and the Illinois*

"what a user has" with "what that user is known to be" in a database narrowly and precisely bridges the gap between the real world and the digital world.[33] This type of identity verification practice has been in use for many decades,[34] but recent advances in immersive technology systems (such as virtual reality gaming or social media services like Meta) and algorithmic analyses create novel privacy concerns that have yet to be squarely addressed by legislatures.[35] The phenomenon of "biometric psychography" describes "the practice of using biometric data to . . . identify a person's interests" by using "behavioral and anatomical information (e.g., pupil dilation) to measure a person's reaction to stimuli over time . . . , reveal[ing] both a person's physical, mental, and emotional state, and the stimuli that caused him or her to enter that state."[36] In the context of marketing, the use of consumer profiles derived from biometric psychographic information may be a dangerously effective advertising tool and ripe for abuse by corporations as yet another discreet proxy in predictive behavioral algorithms used to condition purchasing habits.[37] As technology that facilitates the collection of biometric data becomes increasingly accessible, reliable, convenient, and cheap, its uses will continue to expand beyond marketing. This technology is now "implemented in the human ecosystem at all levels: for a national ID [such as passports], law enforcement, physical access control, border patrol, logical access control . . . and much more."[38]

It is necessary to revisit the legal framework surrounding the collection and use of biometric data by U.S. companies. Although "current thinking around biometrics is focused primarily on identity," novel uses of this data, such as biometric psychography, take the privacy harms associated with biometric data a step further, utilizing such data to identify and potentially capitalize on a person's scientifically-verified interests.[39] Considering how rapidly technology develops and the sensitivity of the data at issue, the regulatory framework must be as nimble and dexterous as the technology itself to be adequately responsive. The regulations

---

Biometric Information Privacy Act as Model Laws?, 38 SANTA CLARA HIGH TECH. L.J. 39, 47–48 (2022). "[H]uman beings can be modeled as potentially informative objects, where biometric information are implied statements about a person." *Id.* This is valuable because such information provides a calculable decrease in the "uncertainty about a person's identity" due to the compiled set of biometric measurements. *Id.* at 48.

33. *See What Is Biometric Authentication?*, *supra* note 29.

34. *See* Joshua D. Jones, *Fingerprint Problems: Laden with Historical Misconceptions*, 18 W. MICH. COOLEY J. PRAC. & CLINICAL L. 199, 202 (2016) (describing how fingerprint database comparisons began as a practice in forensic investigations in the nineteenth century).

35. *See* Brittan Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 VAND. J. ENT. & TECH. L. 1, 27–28 (2020).

36. *Id.* at 27. "[T]hink of traditional biometrics like static images of fingerprint swirls that connect an individual to [their] unique personhood and identity; psychographics, on the other hand, are more akin to consumer profiles that map an individual's buying preferences or shifts in opinion over time." *Id.* at 27–28.

37. *Id.*

38. Jayshree Pandya, *Hacking Our Identity: The Emerging Threats from Biometric Technology*, FORBES (Mar. 9, 2019), https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology.

39. Heller, *supra* note 35, at 27.

also must be capable of review by the federal judiciary if privacy harms relating to biometric data are going to be redressable in our system of adversarial justice.

II. A BRIEF REVIEW OF FEDERAL AND STATE REGULATION OF BIOMETRIC DATA

The United States does not have a generally applicable consumer privacy law.[40] However, the federal government has recognized the need to protect consumer privacy in biometric data by regulating the collection and use of such data in the health insurance and employment contexts.[41] Additionally, the Federal Trade Commission (FTC) has become renowned as an active federal privacy regulator because of its authority to police "unfair or deceptive acts or practices in or affecting commerce."[42] Yet in the case of biometric data, the FTC's regulatory processes come too little too late. Specifically, they fail to address the instantaneous yet life-long harm that characterizes the cavalier collection and use of biometric data by private entities. Such failure undermines Americans' right to privacy and bodily autonomy. Stated differently, once a company has been engaged in a deceptive or unfair trade practice relating to biometrics long enough for the FTC to take regulatory action, the damage has been done, and enforcement at this stage is moot—the victim will live with the consequences for the rest of their life.[43]

State legislatures have been more proactive, enacting statutes that confront biometric data collection in a variety of ways. For example, Arkansas, Connecticut, Iowa, Nebraska, New York, North Carolina, Oregon, Wisconsin, and Wyoming all include biometric information under the definition of "personal information" in their data security breach notification laws.[44] Directly enumerating biometrics in this context serves as an indication of the state legislature's concern about its use in private enterprise. In 2008, Illinois became the first state to enact a statute regulating private enterprise's use of biometric data. Soon after, however, Texas and Washington also enacted statutes that focus on protecting consumers'

40. Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 U. KAN. L. REV. 637, 643–44 (2018).

41. *See* The Genetic Information Nondiscrimination Act (GINA) of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 29 & 42 U.S.C.).

42. *See* 15 U.S.C. § 45(a)(1)–(2). In September 2021, the FTC voted to approve and make public a "series of resolutions that will enable agency staff to efficiently and expeditiously investigate conduct in core FTC priority areas over the next ten years." *FTC Streamlines Consumer Protection and Competition Investigations in Eight Key Enforcement Areas to Enable Higher Caseloads*, FED. TRADE COMM'N (Sept. 14, 2021), https://www.ftc.gov/news-events/press-releases/2021/09/ftc-streamlines-investigations-in-eight-enforcement-areas [hereinafter *FTC Streamlines Investigations*]. One area of law that will be prioritized in the resolution is "Algorithmic and Biometric Bias." *Id.*

43. *See supra* Introduction (discussing how mishandling of biometric data is dangerous in that it is immutable).

44. ARK. CODE ANN. § 4-110-103(7)(E) (2022); CONN. GEN. STAT. § 36a-701b(a)(2)(A)(ix) (2022); IOWA CODE § 715C.1(11)(a)(5) (2022); NEB. REV. STAT. § 87-802(5)(a)(v) (2022); N.Y. STATE TECH. LAW § 208(1)(a)(i)(5) (McKinney 2022); N.C. GEN. STAT. § 75–61(10)(11) (2022); OR. REV. STAT. § 646A.602(12)(a)(v) (2022); WIS. STAT. § 134.98(1)(b)(5) (2022); WYO. STAT. ANN. § 40-12-501 (2022).

biometrics. Each state varies in its approach.[45] Additionally, California's omnibus consumer privacy law, the California Consumer Privacy Act (CCPA), extends a private right of action to California consumers whose biometric information has been subject to data breach.[46] Many of these state laws, such as California's, are also actively developing. The California Privacy Rights Act (CPRA) of 2020 will come into effect in California in January 2023, and it adds "biometric information" to the category of "sensitive personal information" that requires heightened protection, affirmative consent, and informed collection.[47]

A. Federal Regulation

1. The Genetic Information Nondiscrimination Act (GINA)

The closest that federal law comes to regulating the collection of consumers' biometric data is the Genetic Information Nondiscrimination Act (GINA) of 2008.[48] The statute, "[h]ailed as the first civil rights law of the twenty-first century," prohibits health insurance companies and employers from using genetic test results and family medical history to discriminate in their respective industries.[49]

The genetic information that is protected under GINA is defined as (i) genetic test results, (ii) the genetic test results of family members, and (iii) manifested conditions in a person's family members.[50] Title I of the Act prevents health insurance companies from using genetic information in underwriting and rating decisions.[51] The Act amended several federal health insurance laws, deriving its enforcement mechanism from the underlying laws that it modifies.[52] Thus, Title I of GINA is enforced by various agencies such as the Department of Labor, Department of the Treasury, and Department of Health and Human Services.[53]

Title II on the other hand, is a "standalone portion of the federal code with an independent private right of action," that prevents employers from intentionally collecting and using genetic information or family health history in any adverse employment action.[54] Although GINA is one among few U.S. laws featuring a

45. *See* Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14/5 (2022); Capture or Use of Biometric Identifier (CUBI), TEX. BUS. & COM. CODE ANN. § 503.001 (West 2022); WASH. REV. CODE § 19.375.020 (2022).

46. CAL. CIV. CODE §§ 1798.150(a)(1), .81.5(d)(1)(A)(vi) (West 2022).

47. *Id.* § 1798.140(v)(1)(E) (amended 2020).

48. *See* 42 U.S.C. § 2000ff.

49. Bradley A. Areheart & Jessica L. Roberts, *GINA, Big Data, and the Future of Employee Privacy*, 128 YALE L.J. 710, 716 (2019). *See generally* 42 U.S.C. § 2000ff(4)(A)(i)–(iii).

50. 42 U.S.C. § 2000ff(4)(A)(i)–(iii).

51. Areheart & Roberts, *supra* note 49; *see also* Genetic Nondiscrimination in Health Insurance, Pub. L. No. 110-233 (2008) (codified as amended at 29 U.S.C. § 1182 (c)(1)).

52. Jessica L. Roberts, *Preempting Discrimination: Lessons from the Genetic Information Discrimination Act*, 63 VAND. L. REV. 439, 452 (explaining that Title I, like the Health Insurance Portability and Accountability Act (HIPAA) of 1996, amends preexisting insurance regulations by identifying gaps in coverage and expressly addressing them).

53. AMANDA K. SARATA, CONG. RSCH. SERV., RL34584, THE GENETIC INFORMATION NONDISCRIMINATION ACT OF 2008 (GINA) 8, 11–12 (2015).

54. Areheart & Roberts, *supra* note 49, at 717; *see also* 42 U.S.C. § 2000ff-6.

private right of action to vindicate consumer privacy interests, it is infrequently invoked because it has very little applicability and only covers explicit and intentional discrimination, excluding any kind of disparate impact action.[55]

Although discrimination based on genetic information was not a widespread social issue when this law was adopted, Congress sought to "prophylactically address fears about genetic testing by stopping a new form of discrimination before it started."[56] Perhaps Congress's attempt to predict and prevent the as yet undefined contours of genetic discrimination led to GINA's incredibly narrow drafting and application.[57] The limited scope, narrow protected status, and broad exceptions have caused the law to go largely unused.[58] Indeed, although GINA was adopted nearly fifteen years ago with the aim of protecting employees and people seeking insurance from discrimination based on genetic test results, "there have been no such claims in the entirety of GINA's" first ten years in effect.[59]

The few cases that have been brought under GINA for judicial interpretation have established precedent that further narrows the scope of information protected by the law.[60] Most importantly for the purposes of this Comment, courts have held that "biometric screening" information is not "genetic information" under GINA.[61]

In sum, GINA aimed to address a "very specific problem: public anxiety surrounding medical genetic testing."[62] Nearly fifteen years after its inception, commentators frequently dismiss the law "as truncated, ineffective, and even unnecessary."[63] Yet the underlying dangers of corporate entities accessing individuals' biometric data remain and have grown in magnitude exponentially since 2008.[64] Particularly due to the proliferation of technology that utilizes

---

55. Areheart & Roberts, *supra* note 49, at 724–26.

56. *Id.* at 715–16. "Congress crafted the law to deal with the specific risks related to health insurance and employment that could discourage people from seeking genetic testing altogether." *Id.* at 716.

57. *See generally id.* at 724–27 (positing that Congress's intent contributed to GINA's "idiosyncratic protections").

58. *See id.* at 730.

59. *Id.*

60. *See, e.g.*, Ortiz v. City of San Antonio Fire Dep't, 806 F.3d 822, 824, 826 (5th Cir. 2015) (holding that a medical exam required by an employer that tested the employee's blood, vision, lung capacity, chest x-ray, and stress did not fall under "genetic information" as defined by GINA); Fuentes v. City of San Antonio Fire Dep't, 240 F. Supp. 634, 644 (W.D. Tex. 2017) (holding that similar medical tests did not produce genetic information). The statute only covers DNA tests and the directly corresponding medical inferences. *See, e.g.*, *Ortiz*, 806 F. 3d 824.

61. *See Ortiz*, 806 F.3d at 824, 826 (explaining that medical tests that do not have a genetic basis are not subject to GINA's regulation, in fact, very few quanta of biometric data rely on genetic information).

62. Areheart & Roberts, *supra* note 49, at 782.

63. *See, e.g.*, *id.* Though one may argue that this law accomplished the legislature's goal through deterrence out of fear of repercussion, this is unconvincing in the context of the United States' tech industry, where businesses too frequently ask for forgiveness instead of permission when developing products using sensitive data. *See, e.g.*, Miriam A. Cherry, *Are Uber and Transportation Network Companies the Future of Transportation (Law) and Employment (Law)?*, 4 TEX. A&M L. REV. 173, 175 (noting that Uber is one example of a company that frequently asks for forgiveness instead of permission from local authorities). The novel application of BIPA may also be a case on point.

64. *See* Alessandro Mascellino, *Biometric Authentication Use in US Businesses Tripled Over 3 Years to Tackle Cyber Threats*, BIOMETRIC UPDATE.COM (Sept. 21, 2022), https://www.biometric

biometric data, a comprehensive federal law regulating its collection and use is long overdue.

2. The Federal Trade Commission's Authority

The FTC Act is a federal consumer protection law that prohibits "unfair or deceptive commercial practices."[65] Although the Act provides generally-applicable consumer protections, the FTC's "focus on [data] privacy dates back to the enactment of the Fair Credit Reporting Act ('FCRA') in 1970."[66] The Commission has authority to enforce several other sector-specific consumer privacy statutes in addition to FCRA.[67] From the mid-1990's onward, the FTC, acting under the legal authority granted in § 5 of the FTC Act, began examining consumer privacy issues beyond those pertaining to specific sectors ordained by Congress.[68] A deceptive act or practice under the FTC Act must satisfy several elements.[69] The act must be (i) "a representation, omission, or practice"; (ii) "likely to mislead consumers acting reasonably in the circumstances"; and (iii) "material."[70] An unfair act or practice is one that (i) "causes or is likely to cause substantial injury to consumers," (ii) "is not reasonably avoidable by consumers," and (iii) "is not outweighed by countervailing benefits to consumers or to competition."[71]

The FTC has brought a variety of consumer privacy enforcement actions against companies who conducted unfair or deceptive acts and practices by failing to act in accordance with the representations made in their privacy policies,[72] making material changes to their privacy policies without providing adequate notice to consumers,[73] and failing to provide reasonable and appropriate security

update.com/202209/biometric-authentication-use-in-us-businesses-tripled-over-3-years-to-tackle-cyber-threats.

65. 15 U.S.C. § 45(a)(2).

66. Jessica Rich, Comment Letter on Big Data, Consumer Privacy, and the Consumer Bill of Rights, at 1–2 (Aug. 1, 2014), https://www.ftc.gov/system/files/documents/public_statements/573301/140801bigdatacomment.pdf; 15 U.S.C. §§ 1681–1681x. The FTC is the primary enforcer of FCRA, which protects data that is used for decisions involving credit, employment, insurance, and other eligibility determinations "from disclosure to unauthorized persons." Rich, *supra*.

67. *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 & 15 U.S.C.); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506; CAN-SPAM Act, 15 U.S.C. §§ 7701–7713; Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101–6108.

68. Rich, *supra* note 66, at 2; *see also* 15 U.S.C. § 45 (empowering the FTC to take action against unfair or deceptive trade practices broadly).

69. Alexander E. Reicher & Yan Fang, *FTC Privacy and Data Security Enforcement and Guidance Under Section 5*, 25 COMPETITION 89, 89–90 (2016).

70. *Id.*; *see also* Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce 1–2 (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

71. Reicher & Fang, *supra* note 69, at 90; *see also* Letter from FTC Comm'rs to Sen. Wendell H. Ford & Sen. John C. Danforth (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

72. *See, e.g.*, Snapchat, Inc., No. C-4501, 2014 WL 7495798, at *3–6 (F.T.C. Dec. 23, 2014).

73. *See, e.g.*, Facebook, Inc., No. C-4365, 2012 WL 3518628, at *3–6 (F.T.C. July 27, 2012).

measures to protect sensitive consumer information.[74] The FTC has also issued non-binding privacy and data security guidelines as recommended best practice standards for businesses to follow in order to avoid an enforcement action.[75]

Early in 2021, at the joint recommendation of the Bureau of Consumer Protection and the Bureau of Competition, the newly-appointed Commissioners voted and approved a series of compulsory process resolutions, including the expansion of investigative procedures in "algorithmic and biometric bias."[76] They explain that "[c]ompulsory process refers to the issuance of demands for documents and testimony, through the use of civil investigative demands and subpoenas."[77] The Commission also published a series of best practice recommendations for companies using AI and biometric data.[78] The recommendations state that if a business uses AI and biometric data they must "[s]tart with the right foundation," "[w]atch out for discriminatory outcomes," "[e]mbrace transparency and independence," "[a]void exaggerating an algorithm's ability to deliver fair results," "[t]ell the truth about how data is used," "[d]o more good than harm," and "[h]old themselves accountable."[79] These recommendations will necessarily vary widely between enterprises when employed in practice, and such variety will likely make the FTC's enforcement practices unpredictable, slow, and ineffective.

The nature of the FTC's enforcement power allows them to implore businesses to self-regulate in accordance with lofty open-ended best practice recommendations.[80] As a result, "businesses essentially determine[] for themselves the basic rules they will adhere to regarding data collection, use, and disclosure."[81] Best practice policies and slow, reactive enforcement mechanisms may function well in certain privacy contexts but do not effectively protect individuals' biometric data. In the context of biometric data, once there has been a breach and the data is under the control of unknown actors, an irreparable injury has already occurred.

B. State Regulation

The only states that have statutes focusing specifically on the collection and use of biometric data as of the writing of this Comment are Illinois, Texas, and

74. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240–41 (3d Cir. 2015) (holding as a matter of first impression that the FTC's section 5 authority encompasses businesses' cybersecurity practices).

75. *See Business Guidance*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/privacy-security/data-security [https://perma.cc/2MQV-7CCK].

76. *FTC Streamlines Investigations*, *supra* note 42.

77. *Id.*

78. Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FED. TRADE COMM'N (Apr. 19, 2021), https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

79. *Id.*

80. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 604 (2014) (positing how the myriad FTC enforcement actions have come to be respected as a guiding de facto common law).

81. *Id.* The "FTC enforcement added some teeth to the promises in privacy policies, most of which lacked any penalty or consequence if a company failed to live up to its promises." *Id.*

Washington.[82] Although these three statutes are similar in substance (in terms of the scope of entities that must comply and the types of data covered), they have had wildly different effects on the ground. Furthermore, evaluating the timeline when each statute was adopted reveals a shift in corporate awareness of the state's interest in the regulation of biometric data. The level of effectiveness of the state's regulations are contingent upon their enforcement mechanisms and the potential for extraterritorial application.

1. Texas's Capture or Use of Biometric Identifier Statute (CUBI)

In 2009, Texas became the second state, after Illinois, to pass a statute that provided direct protections for consumer biometric data when used by private parties.[83] CUBI requires private organizations to provide notice to individuals and obtain affirmative consent before collecting or using biometric data.[84] Furthermore, the statute prohibits organizations from selling, leasing, or disclosing to third parties any biometric data that was captured for a commercial purpose (unless certain exceptions apply).[85] In addition to providing notice and obtaining consent from consumers, CUBI requires that biometric information collected by companies be stored using "reasonable care" and be deleted within one year of the date it was collected.[86] Notably, CUBI does not provide a private right of action; instead the Attorney General of Texas has the authority to potentially recover $25,000 from companies that are found to be in violation of the statute.[87]

Though litigation under CUBI has been rare, in 2022, the Texas Attorney General brought one of the first cases invoking the law.[88] In its complaint, the AG seeks statutory damages for "billions" of alleged CUBI violations dating as far back as 2011.[89] In addition to damages, the state is seeking injunctive relief in the form of a court order mandating Meta (Facebook's new parent company) to stop

82. 740 ILL. COMP. STAT. 14/5 (2022); BUS. & COM. CODE ANN. § 503.001 (West 2022); WASH. REV. CODE § 19.375.020 (2022). Other states have introduced pending legislation or include biometric information only in laws specifically relating to data breach. *See supra* note 44.

83. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2022); *see also* Carra Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J. L. & POL'Y 769, 791–93 (2018).

84. *See* TEX. BUS. & COM. CODE ANN. § 503.001(c)(1)(A) (West 2022). However, CUBI does not specify the form of notice and consent that the corporate entity must provide to satisfy the statute. *See id.*

85. *Id.* Exceptions to this rule include where the consumer consents to their data being used to identify them in the event of their death or disappearance, where the disclosure completes an authorized financial transaction, or where the disclosure is required under a state or federal warrant issued by law enforcement. *Id.* § 503.001(c)(1)(A)–(D).

86. *Id.* § 503.001(c)(2); *see also* Pope, *supra* note 83, at 792. In this way, CUBI is actually more stringent than Illinois's BIPA, which allows companies to maintain consumer biometric data for three years. *Id.*

87. Pope, *supra* note 83, at 792. There is no maximum cap on fines that can be imposed by the Texas Attorney General for violations of CUBI. *See* TEX. BUS. & COM. CODE ANN. § 503.001(d).

88. F. Mario Trujillo & Jon Frankel, *Texas Starts Enforcing Its Biometric Law*, ZWILLGENBLOG (Mar. 16, 2022), https://www.zwillgen.com/privacy/texas-cubi-law-and-biometric-privacy/ [https://perma.cc/LV5R-8AHX].

89. *See* Plaintiff's Petition at 2–3, State v. Meta Platforms, Inc., No. 22-0121 (filed Feb. 14, 2022).

collecting the covered information in Texas and to delete any information it already had obtained.[90] Although Facebook announced that it has discontinued biometric data collection associated with the "facial recognition" function, the Texas Attorney General argues that this commitment did not extend to the other Meta-owned services and properties.[91]

2. Washington's Biometric Privacy Law

Several years after Illinois and Texas passed laws relating to the collection and use of biometric data by private parties, Washington passed a law on point in 2017.[92] Because BIPA and CUBI had been in effect for over five years by the time that the Washington law first arrived in the state legislature, large corporate firms were already wary of the effects of privacy legislation governing biometric data.[93] Facebook and Google launched major lobbying efforts in opposition to certain aspects of the pending biometric privacy law.[94] The efforts of corporate lobbyists proved to be fruitful; the Washington biometric privacy statute is much friendlier to businesses than the Texas or Illinois statutes.[95] This is because the law is far narrower in scope and also does not have a private right of action.[96] Additionally, the list of covered data which are categorized as "biometric" in the statutory definition notably omits digital photographs and voice audio recordings.[97] Commentators have noted that the strategic exclusion of digital photos and audio recordings makes the Washington law more favorable to tech companies who have long been using business models that have often indiscriminately collected and used these forms of data.[98] Thus, corporate privacy consultants have said that "[s]electing Washington's law as governing user agreements may therefore help

90. *Id.*

91. Jerome Pesenti, *An Update on Our Use of Face Recognition*, META (Nov. 2, 2021), https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/ [https://perma.cc/XJE9-YTSJ]; *see also* Trujillo & Frankel, *supra* note 88.

92. *See* Act of Mar. 2, 2017, ch. 299, 2017 W.A. Laws 1493 (providing consumer protection of biometric data in Washington) (codified at WASH. REV. CODE § 19.375.010–.040 (2022)).

93. *See* Benjamin J. Byer, *Washington's New Biometric Privacy Law: What Businesses Need to Know*, DAVIS WRIGHT TREMAINE LLP (July 24, 2017), https://www.dwt.com/insights/2017/07/washingtons-new-biometric-privacy-law-what-busines (advising companies on how to avoid the consequences of Washington's law on biometric data).

94. Bennett Cyphers et al., *Tech Lobbyists Are Pushing Bad Privacy Bills. Washington State Can, and Must, Do Better*, ELEC. FRONTIERS FOUND. (Mar. 6, 2020), https://www.eff.org/deeplinks/2020/03/tech-lobbyists-are-pushing-bad-privacy-bills-washington-state-can-and-must-do.

95. Byer, *supra* note 93.

96. Cyphers, *supra* note 94.

97. Patel v. Facebook, Inc., 932 F.3d 1264, 1273–75 (9th Cir. 2019), *cert. denied*, 140 S. Ct. 937 (2020). The question of whether digital photographs and voice audio recordings were included under the scope of BIPA was also highly debated until the Ninth Circuit, interpreting Illinois law, confirmed that this information did fall within the definition of biometric data. *See id.*

98. Byer, *supra* note 93. For example, the central dispute in the *Patel* case was whether or not Facebook's "tag your friends" feature used biometric data or not. *Patel*, 932 F.3d at 1270. The court ultimately held that this was a use of biometric data. *Id.* Other companies, who may use similar technology, have to be very careful about which state these services are offered in and how they can comply with the law. *Id.*

companies avoid being subject to any private lawsuits, such as class actions under [BIPA]."[99]

There is no private right of action for violations of the statute, and similar to the Texas statute, Washington's law may be enforced by the attorney general.[100] Additionally, the statute also prevents private lawsuits from being filed against companies directly under most alternative statutory causes of action because it is enforced through the state's Consumer Protection Act, requiring that this remedy be pursued first.[101] Critics argue that Washington's biometric law shows what can happen when technology companies are willing to invest time and massive amounts of money into preventing the enactment of statutes unfavorable to their interests.[102] The corporate lobbying influence on the Washington statute has made it largely ineffective, casting a gloomy shadow over the notion of future state privacy laws governing biometric data collection.

3. Biometric Data Under California's Consumer Privacy Act (CCPA)

Effective January 1, 2020, the California Consumer Privacy Act (CCPA) regulates the collection and processing of personal information that could be used to identify or describe a particular person or household.[103] The law's aim is to comprehensively protect the information of California consumers, "regardless of what sector of the economy the data originated [from]."[104] The CCPA's protections extend to "California consumers," which the law defines as "a natural person who is a California resident."[105] The Act imposes certain duties and obligations on for-profit businesses and partnerships that collect and process California consumers' information.[106] California consumers also have certain affirmative rights that must be respected by covered businesses and partnerships in order for those entities to be in compliance with the CCPA.[107] For example, consumers "have the right to opt out of the sale of their personal information."[108]

The CCPA expressly enumerates biometric data as a category of personal information that is afforded specialized rights and protections.[109] The legislature emphasizes the importance of biometric data's inclusion under this law by intentionally excluding it from the section that exempts publicly available

99. Byer, *supra* note 93; *see also* Sosa v. Onfido, Inc., 8 F.4th 631, 638–40 (7th Cir. 2021) (holding that a third-party biometric verification service provider was not a party to the app's terms of service contract, which contained a choice of law clause selecting Washington's law instead of Illinois's).

100. *See* WASH. REV. CODE § 19.375.020 (2022).

101. Byer, *supra* note 93.

102. Pope, *supra* note 83, at 793.

103. *See* California Consumer Privacy Act (CCPA), CAL. CIV. CODE § 1798.140 (West 2022); Buresh, *supra* note 32, at 63.

104. Buresh, *supra* note 32, at 47.

105. CAL. CIV. CODE § 1798.140(7)(g) (West 2022); *see also* Buresh, *supra* note 32, at 48 ("The statute does not protect the personal information of individuals [who are] temporarily located within California.").

106. Buresh *supra*, note 32, at 65.

107. *See id.* at 63–64.

108. *Id.* at 64.

109. CAL. CIV. CODE § 1798.140(o)(1)(E) (West 2022).

information.[110] Practically speaking, this means that if a business derives biometric information from publicly available images of an individual, this information is still categorized as personal information.[111]

The CCPA has two different forms of penalties for non-compliance. First, the Act imposes penalties for security breaches.[112] Consumers covered by the CCPA are empowered with a private right of action in the case of a data breach involving their personal information.[113] "The Attorney General of California may enforce the privacy provision of the CCPA via civil penalties with a maximum of $7,500 per violation."[114] The Act permits individuals and the attorney general to sue companies at the same time.[115]

The CPRA, which goes into effect in January of 2023, gives California citizens the right to correct inaccurate information and have information collected about them be subject to data minimization and purpose limitations.[116] The CCPA and the CPRA take a revolutionary approach to the regulation of consumer data usage in the private sector. In particular, the rights-based approach of the CPRA recognizes a right to data privacy in the corporate context that is not recognized elsewhere in the United States.[117] Where the CCPA fails is in its reactionary structure of enforcement. Though there is a private right of action granted to consumers, the fact that private suits may be brought only in the context of a data breach is problematic in light of the Supreme Court's standing jurisprudence.[118] Although the language of the statute attempts to address the heightened sensitivity of biometric data by excluding it from the exemption for otherwise "publicly available information," a private right of action that solely responds to data breach is insufficient.[119]

4. Illinois's Biometric Information Privacy Act (BIPA)

The Illinois General Assembly enacted BIPA in 2008 in response to growing public concern about the private use of biometric data "in the business and security

110. *See id.* § 1798.140(o)(2) ("'Publicly available' does not mean biometric information collected by a business about a consumer without the consumer's knowledge.").

111. *See* Buresh, *supra* note 32.

112. *Id.* at 64.

113. *Id.* The damages for a data breach brought by consumers are $750 per violation or actual damages, whichever is greater. *Id.*

114. *Id.*

115. *See* CAL. CIV. CODE § 1798.150 (West 2022) (empowering both citizens and the California Attorney General to pursue violations under the Act).

116. Buresh, *supra* note 32, at 66–68.

117. *See generally id.* (noting that the CCPA shares some of the same privacy principles that were established by the Organization for Economic Co-Operation and Development (OECD) in 1960 as the General Data Protection Regulation (GDPR), which created non-binding ethical principles relating to data collection).

118. *See, e.g.*, TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021); Spokeo v. Robins, 578 U.S. 330 (2016). Specifically, private rights of action for data breach have a hard time establishing Article III standing unless the breached data has actually been used to commit fraud or the plaintiff has incurred actual damages. *See, e.g.*, *TransUnion*, 141 S. Ct. 2190; *Spokeo*, 578 U.S. 330.

119. CAL. CIV. CODE § 1798.140(L)(2) (West 2022).

screening sectors."[120] The assembly expressed concern that Chicago and other locations in Illinois were emerging as "pilot testing sites for new application of biometric facilitated financial transactions."[121] The legislative findings that accompany the statute state that "[t]he full ramifications of biometric technology are not fully known," and that "the public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[122] The use of biometric information has grown significantly in the years since BIPA was enacted.[123] Most frequently, biometric information is used in commerce for employment time management systems, internal corporate security access, identity verification, residential building access permission, and health plans or wellness programs.[124] Yet as the case law develops, the courts have continued to expand the protections afforded by BIPA to increasingly novel circumstances.[125]

BIPA defines biometric identifiers as retina or iris scans, voiceprints, fingerprints, or scans of hand or face geometry.[126] Biometric information, on the other hand, is "any information regardless of how it is captured, converted, stored or shared, based on an individual's biometric identifier used to identify an individual."[127] BIPA only applies to private businesses, nonprofits, and other associations that seek to interact with biometric data of Illinois residents; public sector organizations are expressly exempt.[128] Overall, BIPA contains the following five types of requirements that covered entities must abide by: notification, consent, storage and security, prohibition on profit, and prohibition on non-consensual disclosure.[129]

In practice, the notice requirement means that businesses must develop and make a public written policy establishing the details of their biometric data retention schedule, and that schedule must include guidelines for the permanent destruction of the biometric information either when the "initial purpose for collecting it has been satisfied or within 3 years."[130]

Next, BIPA's consent provision imposes three requirements that must be fulfilled in writing before a company can process biometric data.[131] The company must first inform the individual that their biometric information is going to be

120. Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146, 1149 (7th Cir. 2020).

121. *See id.* (quoting 740 ILL. COMP. STAT. 14/5(a)–(b) (2022)).

122. *Id.* at 1149–50 (quoting 740 ILL. COMP. STAT. § 14/5(f)–(g) (2022)).

123. *See The Illinois Biometric Information Privacy Act (BIPA)*, CASEGUARD (Aug. 27, 2021), https://caseguard.com/articles/the-illinois-biometric-information-privacy-act-bipa-the-first-in-the-us/.

124. *Id.*

125. *See, e.g.*, Patel v. Facebook, Inc., 932 F.3d 1264, 1271–75 (9th Cir. 2019) (holding that Facebook's use of facial scans in users' uploaded photos for Facebook's "find your friends" feature was use of biometric information). The Illinois legislature could not have contemplated such a use because no such feature of Facebook or any other social media networks existed in 2008.

126. 740 ILL. COMP. STAT. 14/10 (2022).

127. *Id.*

128. *Id.* Specifically, the law excludes any "[s]tate or local government agency" or "any court of Illinois, a clerk of the court, or a judge or justice thereof." *Id.*

129. McMahon, *supra* note 25, at 901.

130. 740 ILL. COMP. STAT. 14/15(a) (2022).

131. *See id.* § 14/15(b); *see also* McMahon, *supra* note 25, at 902.

collected.[132] Next, the company must provide written notice to the individual of the purpose for which the biometric information is collected, the length of time that the company will be collecting the data, and how long it will be used and stored.[133] Finally, the company must obtain the individual's written release, executed by the individual whose biometric data is going to be collected.[134]

BIPA prohibits the private entity from profiting off of biometric information. The company collecting biometric information may not "sell, lease, trade or otherwise profit" from biometric data.[135] The "disclos[ure], redisclos[ure], or other[] disseminat[ion]" of an individual's biometric data is prohibited without prior consumer consent,[136] unless the disclosure or redisclosure is necessary to complete a financial transaction that the individual has requested or authorized.[137] BIPA also permits disclosure or redisclosure where required by law or by a valid subpoena or warrant.[138]

Furthermore, BIPA also requires that "reasonable" security requirements (in the context of the implicated industry) be implemented to safeguard the consumer's biometric data when a company stores or transmits data in its possession.[139] The Act requires the company to "store, transmit, and protect" the biometric data in a "manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information."[140]

BIPA has potentially expansive geographic application even though it is an Illinois statute and does not have an extraterritorial provision.[141] Although there is no clear intent expressed by the legislature that the Act should have extraterritorial application (as required by Illinois law), recent jurisprudence has developed surrounding specific personal jurisdiction which may permit extraterritorial applications.[142]

To determine whether it has jurisdiction over a BIPA defendant who is located outside of Illinois, the court engages in a fact-intensive personal jurisdiction analysis.[143] The court uses three "essential requirements" to establish specific personal jurisdiction: (i) the defendants have purposefully availed themselves of the

132. 740 ILL. COMP. STAT. § 14/15(b)(1) (2022).

133. *Id.* § 14/15(b)(2).

134. *Id.* § 14/15(b)(3).

135. *Id.* § 14/15(c). Furthermore, individuals under BIPA do not have the capacity to consent to the sale of their own biometric data. *Id.*

136. *Id.* § 14/15(d).

137. *Id.* § 14/15(d)(1)–(2).

138. *Id.* § 14/15(d)(3)–(4).

139. *Id.* § 14/15(e)(1).

140. *Id.* § 14/15(e)(2).

141. *See* Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *5–6 (N.D. Ill. 2017) (applying Illinois law and noting that the Illinois Supreme Court has held that a statute in Illinois will not have extraterritorial effect unless clearly intended by the legislature, and that none of the express provisions in BIPA indicate clear intent by the legislature for the Act to have extraterritorial application); *see also* 740 ILL. COMP. STAT. §§ 14/1–14/99 (2022).

142. *See Monroy*, 2017 WL 4099846, at *5–6.

143. *See* McGoveran v. Amazon Web Servs., 488 F. Supp. 3d 714, 720–23 (S.D. Ill. 2020); *see also* Mutnick v. Clearview AI, Inc., No. 20 C 0512, 2020 WL 4676667, at *1–3 (N.D. Ill. 2020).

privilege to conduct business or purposefully directed contacts into the forum state, (ii) plaintiffs' injuries result from the defendant's forum-related activities, and (iii) permitting personal jurisdiction would comport with the court's traditional notions of fair play and substantial justice.[144] In the context of online-enterprise and third party contractors, the application of the "minimum contacts" test to establish specific personal jurisdiction has created massive extraterritorial applications of BIPA.[145] Thus, nearly all American online entities that interact with Illinois consumers' biometric data are incentivized to be aware of and comply with BIPA, regardless of their principal place of business.[146]

For example, in *Figueroa v. Kronos Inc.*, the Northern District of Illinois refused to grant the defendant's motion to dismiss in a BIPA action brought against an employment time-clock company that utilized employee biometric data to verify their identity when they clocked in or out.[147] Though the court did not frame its analysis in the context of personal jurisdiction, it explained that the defendant sold its systems to "thousands of employers in Illinois" and that BIPA requires employers who use biometric-based time-keeping tools, and the provider of such tools, to comply with its requirements.[148]

In light of its expansive applicability, the most significant element of BIPA that sets it apart from other privacy laws in the United States is the private right of action that allows for any aggrieved person to recover damages.[149] The alleged violation of any of the above-listed provisions (with particular emphasis on the notification, consent, and disclosure obligations) qualifies as an injury for which an individual plaintiff may seek damages.[150] The statute provides that any aggrieved individual may receive liquidated damages of $1,000 or actual damages, whichever is greater, for each negligent violation.[151] In the case of intentional or reckless violation, the plaintiff is entitled to $5,000 liquidated damages or actual damages, whichever is greater.[152] "BIPA does not define 'intentionally' or 'recklessly.'"[153] The Illinois state courts have chosen to interpret intentionally and recklessly as they

144. *Mutnick*, 2020 WL 4676667, at *2 (citing Lexington Ins. Co. v. Hotai Ins. Co., 938 F.3d 874, 878 (7th Cir. 2019)).

145. *See* Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1100–02 (N.D. Ill. 2017) (holding that personal jurisdiction was proper against a California corporation because the plaintiffs were Illinois citizens, the photos at issue were taken in Illinois, and the photos were uploaded to the cloud from an Illinois IP address); *Monroy*, 2017 WL 4099846, at *6 (holding that personal jurisdiction was conferred where the plaintiff's photos were uploaded to the defendant's website from a device located in Illinois and via an IP address in Illinois).

146. *See, e.g.*, Figueroa v. Kronos Inc., 454 F. Supp. 3d 772, 779, 792 (N.D. Ill. 2020).

147. *Id.*

148. *Id.* at 779, 783. *But see* Bray v. Lathem Time Co., No. 19-3157, 2020 WL 1492742, at *4–5 (C.D. Ill. Mar. 27, 2020) (dismissing claim for lack of personal jurisdiction in a similar suit against a workplace time-keeping system that utilized biometrics because defendant, a Georgia-based company, had no Illinois operations besides advertising their services to third-party employers in Illinois other than plaintiffs).

149. *See* 740 ILL. COMP. STAT. § 14/20 (2022).

150. McMahon, *supra* note 25, at 901–02.

151. 740 ILL. COMP. STAT. § 14/20(1) (2022).

152. *Id.* § 14/20(2).

153. Rogers v. CSX Intermodal Terminals, Inc., 409 F. Supp. 3d 612, 618 (N.D. Ill. 2019).

have appeared in Illinois common law.[154] Though intentional or reckless violation suits have been brought under BIPA, there has not yet been a successful judgment allowing the heightened damages award because no claims have made it to trial.[155]

Regardless of the lack of precedential clarity under the intentional or reckless damages provisions, companies that utilize biometrics have further reason to fret pending the Illinois Supreme Court's ruling on what constitutes an individual "instance" warranting an award of damages.[156] Because a party is "aggrieved" if a company collects biometric data without certain procedural protections, such as a retention or deletion schedule for the data in their privacy policy, each time the company records a fingerprint while their privacy policy was deficient could constitute an "instance." Such would be the case if the Illinois Supreme Court affirms the Illinois Appellate Court by answering the certified question it is currently considering for the Seventh Circuit. Companies therefore potentially face astronomically large judgments under BIPA litigation.[157]

BIPA class action plaintiffs have come into their own as powerful de-facto regulators.[158] Rarely in American law have the states utilized private plaintiffs as an enforcement mechanism for bare procedural violations as is the case here. The law has been developing quickly as creative plaintiffs' counsel have crafted new ways to bring suit in light of novel technology on nearly a weekly basis through the course of 2020 and 2021. Yet BIPA litigation in federal courts has been distinctly marked by divided interpretations of the Article III standing doctrine.

III. DEVELOPING STANDING DOCTRINE UNDER BIPA

A. Article III Standing and Privacy Harms

Article III of the United States Constitution creates a material limit on federal courts, requiring them to only hear actual "cases or controversies."[159] Thus, the

154. *See id.* Intentional conduct is performed with a "desire to cause consequences or at least a substantially certain belief that consequences will result." *Id.* (citing Ziarko v. Soo Line R. Co., 641 N.E.2d 402, 405 (Ill. 1994)). Recklessness denotes actions that show "utter indifference" or "a conscious disregard" for the statutory violation. *Id.* (citing Resolution Tr. Corp. v. Franz, 909 F. Supp. 1128, 1141 (N.D. Ill. 1995)).

155. Steven Grimes & Eric Shinabarger, *Biometric Privacy Litigation: The Next Class Action Battleground*, BLOOMBERG L. (Jan. 9, 2018), https://news.bloomberglaw.com/business-and-practice/biometric-privacy-litigation-the-next-class-action-battleground/. Plaintiffs can seek huge damages awards under this provision, "claiming that each use of biometric information by an organization (e.g., each swipe of a fingerprint to clock an employee in or out) constitutes a separate intentional violation of the law." *Id.*

156. *See* Cothron v. White Castle Sys., Inc., 20 F.4th 1156, 1167 (7th Cir. 2021). After finding the matter to be one of first impression, the *Cothron* court certified the following question to the Illinois Supreme Court: "[d]o section 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?" *Id. But see* Watson v. Legacy Healthcare Fin. Servs., LLC, 2021 IL App (1st) 210279, ¶ 15 (holding that 15(b) claims accrue with "each and every capture and use of [a] plaintiff's fingerprint or hand scan").

157. Cothron v. White Castle Sys., Inc., 477 F. Supp. 3d 723, 733 (N.D. Ill. 2020).

158. *See* Hartzog, *supra* note 16, at 96.

159. U.S. CONST. art. III, § 2, cl. 1.

threshold question that suits brought in federal court must answer in order to confer subject matter jurisdiction is whether or not the claim confers standing.[160] The Supreme Court's current jurisprudence breaks down the elements of standing into three component parts that each must be met in full: (i) an actual injury suffered by the plaintiff, (ii) an injury "that is fairly traceable to the challenged conduct of the defendant," and (iii) an injury "that is likely to be redressed by a favorable judicial decision."[161]

The Court has further clarified the discreet meaning of each of these categories. To meet the "injury in fact" requirement, the plaintiff must have a violation of a "legally protected interest" that is (i) "concrete and particularized" and (ii) "actual or imminent, not 'conjectural' or 'hypothetical.'"[162] Even if the alleged injury is imminent, it also needs to be "*certainly impending* to constitute injury in fact."[163] The supposedly imminent injury cannot merely consist of "[a]llegations of possible future injury."[164]

1. Spokeo v. Robins

In the context of privacy harms, the Supreme Court limited plaintiffs in *Spokeo* by holding that they do not necessarily meet the concrete injury requirement "whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[165] Standing in federal courts for privacy statutes with a private right of action was at an event horizon after that holding; the slogan the Court reverberated in *Spokeo*'s wake was, "no concrete harm, no standing."[166] Although the Court left "concrete injury" up for interpretation, the Ninth Circuit on remand ultimately concluded that the "dissemination of false information in consumer reports can itself constitute a concrete harm."[167] Therefore, as is also the case with the private right of action conferred in the Fair Credit Reporting Act, as seen in *Spokeo*, Article III standing is a relevant defense to BIPA claims that are brought under the reporting and sale violations, namely subsections 15(a) and 15(c).[168] This defense is now likely to materially shift how classes of plaintiffs plead injury for violations under several of BIPA's provisions after *TransUnion v. Ramirez*.

2. TransUnion v. Ramirez

The most recent Supreme Court case on point, *TransUnion v. Ramirez*, markedly narrowed the standard for what may constitute a "concrete harm" under a

160. McMahon, *supra* note 25, at 912.

161. *E.g.*, Spokeo, Inc. v. Robins, 578 U.S. 330, 338 (2016).

162. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

163. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013).

164. *Id.*

165. *Spokeo*, 578 U.S. at 341.

166. *See* Solove & Citron, *supra* note 22, at 64.

167. Robins v. Spokeo, Inc., 867 F.3d 1108, 1114–17 (9th Cir. 2017). The Supreme Court's holding in *Spokeo* is referenced as "*Spokeo I*" and the Ninth Circuit's is "*Spokeo II*" throughout this Comment.

168. McMahon, *supra* note 25, at 911.

statutory violation of a statutorily vested privacy right without showing further injury.[169]

In *TransUnion,* a class of 8,185 plaintiffs sued the credit reporting agency, TransUnion, under FCRA for incorrectly labeling them as possible terrorists on their credit reports.[170] TransUnion subsequently failed to provide the class of plaintiffs with certain paperwork as prescribed by the statute.[171] The violated provisions of FCRA were materially similar to BIPA's subsection 15(a) provision, which confers a legally-recognized injury where the consumer is inadequately informed as to the retention schedule for the biometric data or when the data is inadequately stored and handled.[172] Specifically, the three requirements from FCRA at issue in *TransUnion* required consumer reporting entities to (i) "follow reasonable procedures to assure maximum possible accuracy" in the credit reports, (ii) provide to the consumer on request "all information in the consumer's file at the time of the request," and (iii) provide a written "summary of rights" prepared by the Consumer Financial Bureau when the consumer requests their file.[173] Under FCRA, plaintiffs have a private right of action whenever a qualifying entity "'willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer . . . ' for actual damages or for statutory damages not less than $100 and not more than $1,000" in addition to attorneys' fees and punitive damages.[174]

In this case, TransUnion, a world-renowned credit-reporting agency, incorrectly labeled thousands of law-abiding Americans as "terrorists, drug-traffickers, or serious criminals" on their credit reports because they just so happen to share first and last names with people on the U.S. Treasury Department Office of Foreign Asset Control list of nefarious actors identified as threats to national security.[175] After discovering this error, many consumers requested their profiles to ensure that they were not among those accidentally labeled as a terrorist on their credit report.[176] TransUnion furnished the reports to the requesting consumers, and although the consumers' names *were* on the list of terrorists in TransUnion's database, the communications the consumers initially received did not reflect this information.[177] Additionally, the plaintiffs complained that when they requested their files, TransUnion also failed to send them the written summary of rights prepared by the Consumer Financial Bureau that, among other things, informed them of possible remedies and of their right to sue.[178] Following a trial, in which the court entered a judgment in favor of the massive class of plaintiffs, a jury

169. *See* Solove & Citron, *supra* note 22, at 65.

170. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2191 (2021).

171. *See* Solove & Citron, *supra* note 22, at 63; *see also TransUnion*, 141 S. Ct. at 2200–01.

172. *See* 15 U.S.C. §§ 1681–1681x *et seq*.

173. *TransUnion*, 141 S. Ct. at 2200–01; *see also* 15 U.S.C. §§ 1681e(b), g(a)(1), g(c)(2).

174. *TransUnion*, 141 S. Ct. at 2201.

175. *Id.* For example, the class representative, Sergio Ramirez, happened to also have the first and last name of a known international nefarious actor. *Id.*

176. *See id.*

177. *Id.*

178. *Id.* at 2202.

awarded the class total damages in excess of $60 million.[179] The Ninth Circuit affirmed the district court, holding that all class members had Article III standing to recover for all three claims, although it reduced the total damages award to $40 million.[180] The Supreme Court granted certiorari to consider whether all of the 8,185 class members had Article III standing as to their three claims.[181]

Justice Kavanaugh, writing for the majority, stated that a vast majority of the class members did not have standing to sue.[182] The Court was unwilling to recognize that plaintiffs had a personal stake in the case when they did not show that their inaccurate credit reports had actually been sent to a third party.[183] Thus, the plaintiffs were unable to demonstrate "concrete harm."[184]

The Court analogized the harm at issue to environmental pollution, where a plaintiff's physical proximity to the legal infraction is directly correlated to the "concreteness" of its injury.[185] A plaintiff in Maine could sue a nearby factory for polluting their land, but a plaintiff in Hawaii would not have standing to sue the same factory because the factory's pollution would not have personally harmed the Hawaii plaintiff.[186] Though federal environmental protection laws may afford both hypothetical plaintiffs a cause of action to sue and statutory damages, Article III standing would distinguish the injury in the two scenarios. The first suit could proceed because the plaintiff would have suffered physical damage to their land. The second lawsuit could not proceed because the plaintiff could not show that they "suffered any physical, monetary, or cognizable intangible harm traditionally recognized as providing a basis for a lawsuit in American courts."[187]

The concurrence continued by explaining that "[a]n uninjured plaintiff who sues in those circumstances is, by definition, not seeking to remedy any harm to herself but instead is merely seeking to ensure a defendant's 'compliance with regulatory law' (and, of course, to obtain some money via the statutory damages)."[188] The Court referred to the various intangible harms that *have* traditionally been recognized as providing a basis for lawsuits in American courts, including "reputational harms, disclosure of private information, and intrusion upon seclusion."[189]

Though the Court's analogy may offer a patriotic exercise in visualizing the rolling hills of our great green republic, the hypothetical is not analogous to this case—a data breach by a Maine company may well affect a citizen in Hawaii as immediately and poignantly as it would a Mainer. Such is the nature of the internet. Clearly, where the legislature has created a private right of action for a violation of an affirmative disclosure requirement, that harm is as concrete, actual,

179. *Id.*
180. *Id.*
181. *Id.* at 2202–03.
182. *Id.* at 2214.
183. *Id.*
184. *Id.* at 2203, 2210.
185. *Id.* at 2205–06.
186. *Id.* at 2206.
187. *Id.*
188. *Id.* (quoting Spokeo v. Robins, 578 U.S. 330, 345 (2016) (Thomas, J., concurring)).
189. *Id.* at 2204.

and particularized to the individual citizen as it is to society writ large (it is their personal biometrics at stake after all). To say otherwise is to misconstrue the law in the name of covert gatekeeping operations for corporate benefit flying under the flag of artificially inflated notions of "traditional justice."

B. Standing in BIPA Suits

BIPA litigation has been a phenomenon of only the last fifteen years, even though it was enacted in 2008.[190] The frequency of litigation has been snowballing over the past few years; plaintiffs have brought over three hundred suits in a variety of contexts.[191] BIPA litigation has generally fallen within one of two broad industries: "employment cases and consumer-technology cases."[192] The employment cases have generally involved plaintiff-employees suing companies that provide time-keeping systems that record when an employee clocks in or out (for example, through the use of a fingerprint).[193] The other category, consumer-technology cases, involves media services such as social media, immersive videos games, or photo-sharing services, but has also been extended to include "vending machines and tanning salons, [that] use the biometric information and/or identifiers of their users."[194] The extraterritorial application of BIPA under the Illinois' Supreme Court's interpretation of personal jurisdiction in conjunction with the Class Action Fairness Act (CAFA) has allowed classes of plaintiffs to bring actions against (sometimes massive) out-of-state corporations with minimal diversity.[195]

1. Rosenbach v. Six Flags Entertainment Corp.

Illinois case law has clearly stated that statutory standing under BIPA is conferred when plaintiffs plead pure procedural violation of the statute without the need to show additional damages.[196] This doctrine was established by the Illinois Supreme Court in the landmark 2019 case, *Rosenbach v. Six Flags Entertainment Corp.*[197] In *Rosenbach*, an Illinois Six Flags sold repeat-entry admission passes by scanning pass-holders' fingerprints, recording and storing their information.[198] Six Flags would use the fingerprints to quickly verify the customers' identity the next time they visited.[199] Plaintiff Rosenbach sued on behalf of her minor son and a class of similarly situated plaintiffs, who had received season passes while on a

190. *See* Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015) (stating that the Court was "unaware of any judicial interpretation of [BIPA]" in 2015).

191. McMahon, *supra* note 25, at 908.

192. *Id.*

193. *See, e.g.*, Figueroa v. Kronos Inc., 454 F. Supp. 3d 772, 779 (N.D. Ill. 2020); Cothron v. White Castle Sys., Inc., 20 F.4th 1156, 1159 (7th Cir. 2021).

194. McMahon, *supra* note 25, at 909.

195. *See* 28 U.S.C. § 1453(c)(1); *see also Cothron*, 20 F.4th at 1159.

196. *See supra* Section II.B.4.

197. *See* Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶ 2.

198. *Id.*

199. *Id.* Six Flags argued in its response to the complaint that this procedure made entry to the park "faster and more seamless," that it would "maximize[] the time pass holders [were] in the park spending money," and that it "eliminate[d] lost revenue due to fraud or [shared passes]." *Id.*

school field trip and submitted to the fingerprinting procedure.[200] However, they were not provided any informative paperwork nor had their guardians been asked to sign any consent forms relating to the collection of their biometric data.[201] The complaint alleged violation of three provisions of BIPA: (i) Six Flags collected, captured, stored, or obtained biometric information without informing them (or their authorized representatives); (ii) Six Flags failed to inform the consumer in writing of how long and for what purpose the biometric information was being collected and stored; and (iii) Six Flags failed to obtain a written release from the consumer authorizing such collection, use, and storage.[202] The primary injury pled was the fact that the defendant's actions violated the statute.[203]

On interlocutory appeal from a denial of standing in the lower courts, the Supreme Court of Illinois determined that "when a private entity fails to comply with one of [BIPA's] requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach."[204] More broadly, this means that "such a person . . . would clearly be 'aggrieved' within the meaning of [BIPA]."[205] The court did not stop there. It continued by saying that "[n]o additional consequences need be pleaded or proved" and that "[t]he violation, in itself, is sufficient to support the individual's or customer's statutory cause of action."[206] This ruling clarified that a violation of the procedural provisions in section 15 qualified as a sufficiently significant injury to be redressed in Illinois courts.[207] Indeed, the *Rosenbach* court emphasized the significance of the fact that, through BIPA, the Illinois "General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information."[208] After invoking several methods of statutory interpretation, the Illinois Supreme Court arrived at this conclusion by evaluating the term "aggrieved" in the context of other similar statutes and other areas of the common law where the term has been used in analogous circumstances.[209]

The defendant argued that BIPA's use of the term "aggrieved," left undefined in the statute, is determinative of the plaintiff's injury when no further injury is pled.[210] The defendant argued that where the legislature has made expressly clear where it intends to confer a private right of action without proof of additional injury, as it did in the Illinois Consumer Fraud and Deceptive Business Practices Act.[211]

---

200. *Id.*
201. *Id.* at ¶¶ 7–8.
202. *Id.* at ¶¶ 10-12.
203. *Id.*
204. *Id.*
205. *Id.* at ¶ 33.
206. *Id.*
207. McMahon, *supra* note 25, at 912.
208. *Rosenbach*, 2019 IL 123186, ¶ 33. This suggests that the Illinois legislature sought to confer a practically proprietary right to individuals over their biometric data. *See id.*
209. *See id.* at ¶¶ 22–36.
210. *See id.* at ¶¶ 37–38.
211. *Id.* at ¶ 21; *see also* 815 ILL. COMP. STAT. 505/10a(a) (2022).

The court rejected this argument, instead likening BIPA more closely to the AIDS Confidentiality Act,[212] in which the legislature also left the word "aggrieved" undefined in the statute, and authorized a private right of action without necessitating proof of actual damages to recover.[213] In this context, the court reasoned that the lack of an expressly articulated requirement that the plaintiff show additional harm was *not* dispositive of the issue when the "popularly understood meaning" of aggrieved may be easily determined.[214] The court drew its popularly understood definition of the word "aggrieved" from a hundred-year-old case, finding that it "means having a substantial grievance; [which is] a denial of some personal or property right."[215] The *Rosenbach* court found that a person would fall under this definition if "[their] legal right [was] invaded by the act complained of *or* [their] pecuniary interest [was] directly affected by the decree or judgment."[216] Accordingly, the court concluded that, based on the intent of the legislature, a person's legal, personal, or property interests were infringed upon by a bare violation of the statute, without the need to show additional injury.[217]

In reaching this conclusion, the court refuted the lower court's characterization of these statutory violations as "merely 'technical' in nature."[218] The court stated that this characterization "misapprehends the nature of the harm [the] legislature is attempting to combat."[219] BIPA gives individuals the right to control their biometric information by giving them the power to withhold consent to its use and collection.[220] These disputed procedural protections are "particularly crucial" to achieving the protective goal because today's digital world promotes the "wholesale collection and storage" of individuals' biometric data.[221]

The distinction between the characterizations of BIPA injuries is important and informative. The *Rosenbach* court reversed the lower court's articulation of the privacy harm at the heart of BIPA and found it to be peculiarly personal and almost proprietary. This legally vested right is most akin to the privacy right to be let alone.[222] The focus of the Illinois legislature was on the individual's inherent right to control their biometric information and the recognition that a prophylactic protection was integral to achieving this goal. This is clearly the correct interpretation of BIPA.

212. *See* 410 ILL. COMP. STAT. 305/1–/16 (2022).

213. *Rosenbach*, 2019 IL 123186, ¶ 26 (citing Doe v. Chand, 781 N.E.2d 340, 351 (Ill. App. Ct. 2002)).

214. *Id.* at ¶ 29.

215. *Id.* at ¶ 30 (quoting Glos v. People, 102 N.E. 763, 766 (Ill. 1913)).

216. *Id.* (emphasis added by the *Rosenbach* court) (quoting *Glos*, 102 N.E. at 766).

217. *Id.* at ¶ 33.

218. *Id.* at ¶ 34 (quoting Rosenbach v. Six Flags Ent. Corp., 2017 IL App (2d) 170317, ¶ 23).

219. *Id.*

220. *Id.*

221. *Id.*

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

2. Bryant v. Compass Group USA, Inc.

Shortly thereafter, on materially similar facts, the Seventh Circuit considered whether BIPA violations are sufficient to support Article III standing in federal court as a matter of first impression in *Bryant v. Compass Group USA, Inc.*[223] While both *Rosenbach* and *Bryant* allowed easier access for BIPA actions in state court, the Seventh Circuit, in interpreting Illinois law, mischaracterized the precise injury articulated in *Rosenbach* by comparing it to the *informational* privacy harm from FCRA. The harm at the heart of BIPA is more akin to the right to privacy in one's bodily autonomy. Yet the Seventh Circuit noted that "standing requirements in Illinois courts are more lenient than those imposed by Article III."[224]

In *Bryant*, the class representative, Christine Bryant, worked at a call center in Illinois that had a workplace cafeteria that featured "Smart Market" vending machines owned and operated by Compass Group.[225] The vending machines did not accept cash; instead users were instructed to create an account linking their fingerprint to their bank account to purchase items.[226] The plaintiff brought suit under BIPA complaining that Compass Group never publicly made a retention and data destruction schedule for the data it was collecting and storing.[227] In relation to the plaintiff specifically, Compass failed to inform Bryant in writing that her fingerprint was collected and stored; inform her of the specific purpose and length of time it would be stored for; and obtain her written release to collect, store, and use her fingerprint in the first place.[228]

Compass removed the action to federal court under the Class Action Fairness Act (CAFA) because the parties were diverse and the amount in controversy exceeded five million.[229] Once in federal court, Bryant moved to remand to state court for lack of subject matter jurisdiction.[230] She had crafted her complaint with the goal of remaining in state court, arguing on removal that the class specifically lacked the "concrete injury-in-fact necessary to satisfy the federal requirement."[231] In challenging the district court's grant of remand, the defendant had the burden of establishing the plaintiff's Article III standing.[232]

Compass, borrowing language and reasoning from *Rosenbach*, emphasized that BIPA "has elevated to protectible status a person's inherent right to control her own body, including the associated biometric identifiers and information."[233] Therefore, under Compass' theory of the case, any violation or trespass on that legally created right is a significant injury-in-fact.[234] The court disagreed.[235]

---

223. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 622 (7th Cir. 2020).

224. *Id.*

225. *Id.* at 619.

226. *Id.*

227. *Id.*

228. *Id.* at 622. These are alleged violations of subsections 15(a) and (b) of BIPA. *Id.*

229. *Id.* at 620; *see also* 28 U.S.C. § 1332(d).

230. *Bryant*, 958 F.3d at 620.

231. *Id.* The district court agreed, and the case arrived at the Seventh Circuit on interlocutory appeal of the district court's remand. *Id.*

232. *Id.*

233. *Id.* at 621.

234. *Id.*

After walking through the few other federal cases that directly confronted this issue, the *Bryant* court was satisfied to analogize standing under BIPA to standing in the private right of action conferred in FCRA, which at the time, had most recently been evaluated in *Spokeo.*[236] The Seventh Circuit found Justice Thomas's concurrence in *Spokeo* particularly informative for the analysis.[237] In his concurrence, Justice Thomas distinguished between two types of *informational* injuries: one "arises when a private plaintiff asserts a violation of her own rights; the second occurs when a private plaintiff seeks to vindicate public rights."[238] For the first category of vindicating a plaintiff's "personal rights," he provided the examples of actions for "trespass, infringement of intellectual property rights, and unjust enrichment."[239] He then pointed to actions to "abate a public nuisance[] or disputes over the use of public land" to illuminate the latter "public right."[240]

The Seventh Circuit then found that the class plaintiff could have standing where she asserted a violation of her own "personal rights" under the statute.[241] For example, Bryant had standing to sue under subsection 15(b) for the use of her fingerprints absent informed consent without the need to show "further tangible consequence."[242] However, she did not have standing to sue under section 15(a), which requires the company to publicly disclose their collection and retention schedule for biometric data.[243]

In justifying the division between these interpretations, the court incorrectly characterized *Rosenbach*'s analysis of BIPA's legally vested injury, specifically those rights established in subsection 15(b). The *Bryant* court claimed that the purpose of the statute is to provide an effective notice-and-consent regime "to ensure that consumers understand, before providing their biometric data, how that information will be used" so that they might have a meaningful choice before engaging with the company's services or taking their business elsewhere.[244] The court insisted that this is not a superfluous requirement because the privacy policy, delivered to the individual and mandated by the statute, provides material information to the individual with regards to their ability to provide informed consent in the transaction.[245]

The injury in *Bryant* was mischaracterized because BIPA clearly ventures beyond the notice-and-consent regime that has been a marked characteristic of United States consumer privacy law. The court's first mistake was likening BIPA's cause of action to the private right of action under FCRA because the nature of the injury in BIPA is different than FCRA. The procedural aspects of BIPA are significantly more important than the procedural aspects of FCRA in

235. *Id.* at 622.
236. *Id.* at 623.
237. *Id.* at 624.
238. *Id.*
239. *Id.*
240. *Id.*
241. *Id.*
242. *Id.*
243. *Id.* at 626.
244. *Id.*
245. *Id.*

protecting the core right that each statute preserves. As Justice Thomas elucidated in his concurrence in *Spokeo*, the injury at the heart of FCRA's private right of action is similar to informational injury, like infringement of copyright or trespass to property. This is materially distinct from the intimate right to bodily autonomy that lives at the heart of BIPA described by the Illinois Supreme Court. Splitting the harms into public and private, as would be appropriate for private versus public nuisance, has led courts to functionally eliminate a successful and creative mechanism for the enforcement of privacy protections.

The nominally discrete difference in injury recognized by the federal courts is deleterious to the efficacy of BIPA. After the landmark decisions in *Rosenbach* and *Bryant*, plaintiffs filed more federal "BIPA claims in 2020 . . . than in 2018 and 2019 combined."[246] The difference between the permissive standing in Illinois state court and the stricter standard in federal courts has created a deeply divided battleground. "[A] review of Illinois federal district court dockets from November 2020 through January 2021[] revealed only [twelve] BIPA complaints filed in federal court, but at least [thirty-six] removed from state courts . . . ."[247] Once the case has successfully been removed, the defendants will likely move to dismiss BIPA actions from federal court for lack of subject matter jurisdiction.[248] Historically, standing to sue in the context of violations of privacy has been a formidable obstacle, particularly where the plaintiff class suffers no pecuniary harm, though they may suffer a clear violation of a legally recognized privacy harm.[249] The battle for standing in BIPA litigation effectively deprives plaintiffs of a federal forum for redress and unduly delays recovery because of protracted litigation and the increased cost of pursuing a suit in distant venues such as California, where many tech companies are located. In the context of providing protections for biometric data, this delay and expense is devastating.

IV. ARTICULATING THE INJURY

Following *Bryant*, the Seventh Circuit and several other courts continued to distinguish the private and public informational duties owed by covered entities, in order to find Article III standing in several other provisions of BIPA.[250] Because

246. Jennifer Marsh, *Analysis: 7th Circuit's BIPA Rulings Provide State Court Roadmap*, BLOOMBERG L. (Feb. 18, 2021), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-7th-circuits-bipa-rulings-provide-state-court-roadmap.

247. *Id.* This data indicates that "defendants are steering cases to federal court more often than plaintiffs are filing them there." *Id.*

248. McMahon, *supra* note 25, at 911.

249. Margot E. Kaminiski, *Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation*, 66 DEPAUL L. REV. 413, 414 (2017). "As one court explained, 'even though injury-in-fact may not generally be Mount Everest . . . in data privacy cases . . . the doctrine might still reasonably be described as Kilimanjaro.'" *Id.* (quoting *In re* Google Inc. Priv. Pol'y Litig., 2013 WL 6248499, at *4 (N.D. Cal. Dec. 3, 2013)).

250. *See, e.g.*, Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146, 1154–55 (7th Cir. 2020) (holding that section 15(a) of BIPA's requirement that a covered entity adhere to their publicly stated use and purpose for collecting biometric data conferred standing); Cothron v. White Castle Sys., Inc., 20 F.4th 1156, 1161 (7th Cir. 2021) (holding that the unlawful retention of biometric data, similar to its unlawful collection, confers Article III standing). *But see* Thornley v. Clearview AI, Inc., 984 F.3d

sections 15(a) (conferring a right of action where a company fails to publish a data retention and deletion schedule) and 15(c) (which generally prohibits the subsequent sale of biometric information) are the most likely subsections to be the cause for denial of standing, this Comment focuses on those two sections specifically.

The Ninth Circuit recently utilized a particularly informative two-part test, developed in *Spokeo II*, to evaluate the propriety of BIPA standing in *Patel v. Facebook*.[251] The Ninth Circuit's reasoning illustrates the Circuit Courts' and Supreme Court's problematic characterization of the nature of the injury conferred by the Illinois legislature, as seen and articulated above in *Rosenbach.*

In *Patel,* the court considered two issues to evaluate standing for a BIPA claim: "whether the statutory provisions at issue were established to protect [the plaintiff's] concrete interests (as opposed to purely procedural rights), and if so, whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests."[252]

To illustrate the principle at the heart of each step of the analysis, the court first used a case conferring standing under the Telephone Consumer Protection Act (TCPA).[253] The court explained that the statutory provision, which gave consumers a private right of action where a company texted or called a consumer without his or her consent, "was established to protect the plaintiff's substantive right to privacy, namely the right to be free from unsolicited telemarketing."[254] Because TCPA sought to protect the recognized right to be let alone (free from harassing phone calls) the statutory provision created to preserve this substantive right was sufficient to confer Article III standing.[255]

In contrast, for "step two" of the analysis, the Ninth Circuit referred to a case that did not find standing under a portion of FCRA.[256] In *Bassett v. ABM Parking Services, Inc.*,[257] where a plaintiff sought to sue a parking garage for displaying his credit card's full expiration date on a receipt, the Ninth Circuit refused to find standing without additional alleged injury.[258] The court noted that "even if . . . FCRA created a substantive right to the 'nondisclosure of a consumer's private financial information to identity thieves,' the parking garage's failure to redact the credit card's expiration date did not impact this substantive right" because no one other than the plaintiff himself actually saw the information.[259] Because the substantive right ostensibly protected by FCRA is not preserved if it is not proven that another person viewed the protected information, the court concluded that

1241, 1247 (7th Cir. 2021) (holding that violation of section 15(c)'s general prohibition on the sale of biometric data does not confer Article III standing).

251. Patel v. Facebook, Inc., 932 F.3d 1264, 1270 (9th Cir. 2019).

252. *Id.* (quoting Robins v. Spokeo, Inc., 867 F.3d 1108, 1113 (9th Cir. 2017)).

253. *Id.* at 1271.

254. *Id.* (citing Van Patten v. Vertical Fitness Grp., LLC, 847 F.3d 1037, 1041 (9th Cir. 2017)).

255. *Id.*

256. *Id.*

257. Bassett v. ABM Parking Servs., Inc., 883 F.3d 776, 777 (9th Cir. 2018).

258. *Id.*

259. *Patel*, 932 F.3d at 1271 (quoting *Bassett*, 883 F.3d at 782–83).

standing was not satisfied.[260] The *Patel* court's two-step analysis and discussion of analogous cases inform how a class of plaintiffs should structure their BIPA complaint to survive Article III standing after *TransUnion* and clarify how courts have and will approach harms analogous to FCRA.

The first hurdle that BIPA plaintiffs must clear may be the easiest. Plaintiffs must show that the private right of action was established to protect their concrete interests, as opposed to a purely procedural right.[261] The Supreme Court itself agrees that "[p]rivacy rights have long been regarded 'as providing a basis for a lawsuit in English or American courts.'"[262] Indeed, privacy rights were first articulated by Warren and Brandeis in 1890 when they reviewed over 150 years of relevant case law and identified "a general right to privacy," which developed out of various property and defamation actions in conjunction with novel technological developments such as the portable camera.[263] The privacy torts, which grew from the right to privacy originally articulated by Warren and Brandeis, were informally codified in the Second Restatement of Torts.[264]

The Constitution also confers a right to privacy, though this right varies by degree and context.[265] Developing technology has caused courts to re-evaluate the applicability of tried-and-true legal privacy protections, but the core right to privacy has not wavered.[266] From this history, the Ninth Circuit in *Patel* was able to conclude that "an invasion of an individual's biometric privacy rights 'has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.'"[267] The common-law privacy torts, the commonly understood literal interpretations of privacy, and the slightly more amorphous Constitutional privacy cases, all clearly indicate that the American individual has a well-established right to control "information concerning his or her person."[268]

Yet not all privacy rights are created equal in the eyes of the Court, as evidenced by *TransUnion,* where it was insufficient for standing purposes that

---

260. *Id.*

261. *Id.* at 1272.

262. *Id.* at 1271 (quoting Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016)).

263. *See* Warren & Brandeis, *supra* note 222.

264. RESTATEMENT (SECOND) OF TORTS § 652A (AM. L. INST. 1977). "[T]he existence of a right to privacy [is] recognized in the great majority of the American jurisdictions that have considered the question." *Id.* § 652A cmt. a.

265. *See, e.g.*, NAACP v. Alabama, 357 U.S. 449, 466 (1958) (holding that the First Amendment protected the privacy of political membership); Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (holding that the Fourth Amendment protects individuals' right to privacy from warrantless government searches of their cell-site location data regardless of third-party handlers); Griswold v. Connecticut, 381 U.S. 479, 483 (1965) (holding that the right to privacy emanates from the "penumbras" of the expressly enumerated rights in the Constitution); Obergefell v. Hodges, 576 U.S. 644, 645 (2015) (holding that the Due Process Clause of the Fourteenth Amendment's protections extend to freedom to make personal choices of self-determination, including autonomy and dignity).

266. *See* United States v. Jones, 565 U.S. 400, 416–18 (2012) (Sotomayor, J., concurring) (discussing the novel invasions of privacy caused by developing technology in the context of warrantless government surveillance through the use of a GPS tracking device).

267. *Patel*, 932 F.3d at 1273 (quoting *Spokeo*, 578 U.S. at 341).

268. *Id.* (quoting U.S. Dep't of Just. v. Reps. Comm. for Freedom of Press, 489 U.S. 749, 763 (1989)).

TransUnion merely labeled a plaintiff as a terrorist without also disseminating the report. A minority of the Court characterized the protected privacy right as a reputational one, similar to the right underlying the tort of defamation or libel.[269] As explained above, federal courts addressing BIPA claims have incorrectly analogized the substantive right underlying BIPA to the same "reputational" or "intellectual" one that underlies defamation or copyright infringement.[270] Thus, the first step in articulating a BIPA claim to survive Article III standing is to couch the complaint in the context of privacy rights that have been revered as deserving higher levels of legal protection.

It is clear from the Illinois legislature's commentary, as well as from *Rosenbach* and its progeny, that the substantive right that BIPA attempts to protect is not analogous to an "intellectual" or "reputational" right, but more closely resembles one's right to self-determination and physical autonomy. Plaintiffs should cite to *Rosenbach*, which analogized the protections provided under BIPA to the right under the state's AIDS Confidentiality Act.[271] Additionally, looking to the history of federal defendants who have carefully (if ironically) attempted to plead the same issue will be helpful in this endeavor.[272] If plaintiffs place higher emphasis on the intensely personal and immutable nature of biometric data as a non-fungible extension of the body with the capacity to exist in the digital ether in perpetuity, then they have a better chance of being able to sue in federal court.

The second hurdle to clear may be more challenging. Plaintiffs must plead that the specific procedural violations alleged "actually harm, or present a material risk of harm to" this underlying substantive interest.[273] Like in causation, the plaintiffs must argue in the complaint that their substantive right would be impinged if the defendant did not adhere to the procedural mandates of the law.[274]

As to the requirement set forth in subsection 15(a), whereby defendants must maintain a public retention schedule and a deadline for destroying biometric identifiers in their privacy policy, failure to meaningfully inform consumers of data handling practices nullifies their right to meaningfully consent. In *Rosenbach*, the Illinois Supreme Court explained that the procedural protections in BIPA "are particularly crucial in our digital world [because] when a private entity fails to adhere to statutory procedures . . . the right of the individual to maintain [their] biometric privacy vanishes into thin air."[275] Furthermore, the injury is individualized and differs from a "public nuisance" precisely because the handling of biometric information is unique and peculiarly "concrete." Thus, a failure to adhere to best-handling practices and disclosure requirements mandated by a legislature deprives a plaintiff in Maine or Hawaii of their ability to have meaningful control over and a valid right to privacy in their biometric information as an extension of their body.

---

269. *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2222 (2021) (Thomas, J., dissenting).

270. *See supra* Part III.

271. *See* Rosenbach v. Six Flags Ent. Corp., 2019 IL 123186, ¶¶ 25–27. However, plaintiffs may wish to tread carefully with this analogy to not conflate it with reputational rights.

272. *See generally* Bryant v. Compass Grp. USA, 958 F.3d 617 (7th Cir. 2020).

273. *Patel*, 932 F.3d at 1274 (quoting Robins v. Spokeo Inc., 867 F.3d 1108, 1113 (9th Cir. 2017)).

274. *See id.* at 1273–74.

275. *Rosenbach*, 2019 IL 123186, ¶ 34 (quoting *Patel*, 290 F. Supp. 3d at 954).

As to subsection 15(c), which generally prohibits the sale or forward-transfer of biometric data (plaintiffs do not have the ability to consent to this), the result is the same—this too, deprives the plaintiff of the meaningful autonomous control that is meant to be vindicated through BIPA's notice and consent apparatus.

The Seventh Circuit, while denying standing under this provision in *Thornley v. Clearview AI, Inc.*,[276] suggested that to be successful for the purposes of standing under 15(c), a plaintiff might assert that the collector "has deprived her of the opportunity to profit from her biometric information."[277] This argument actually works against plaintiffs because if it were followed to its logical end, it would imply that one has the right to sell or profit from their body or biological material. It is established law (as well as a matter of good public policy) that one may not do this.[278] The more tenable argument to be made, which was suggested by the majority in *Thornley*, is that "the act of selling [the plaintiff's] data amplified the invasion of her privacy that occurred when the data was first collected, by disseminating it to some unspecified number of other people."[279] If the substantive right conferred by the legislature is of such elevated merit, similar to the right to control one's own body, then violation of the legislative protections through the subsequent dissemination and use of this information for profit clearly is abhorrent to this right. The more that a plaintiff can liken the underlying violation of the law to the data collector selling and profiting from their biological material absent material consent, the more likely they will clear the second hurdle to gain Article III standing.

CONCLUSION

The vacuum created by the lack of a comprehensive federal privacy regime has allowed states to truly show their patchwork of creative solutions as "laboratories of democracy." Many scholars have noted that essentially all privacy stakeholders support the concept of a federal privacy regulation for a variety of reasons.[280] Unfortunately, the failure to act has led to serious lapses in efficacy where even slight deviations from a regulatory protocol in the context of privacy harms can defeat the purpose of the regulation.

State privacy laws, such as BIPA, seek to explore creative remedies to the lack-luster system of redress provided by regulatory agencies. BIPA's private right of action, when enforced as intended, has proven to be an incredibly effective (and growing) enforcement mechanism. In fact, several scholars have referred to BIPA as *the* most important biometric information privacy law currently operating in the United States.[281] BIPA seeks to achieve what has recently been pronounced as best-practices for the handling of biometric data; it requires that companies "start with the right foundation, watch out for discriminatory outcomes, embrace transparency and independence," tell the truth about how data is used, "do more

276. Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1248 (7th Cir. 2021).
277. *Id.* at 1247.
278. *See generally* Moore v. Regents of Univ. of Cal., 793 P.2d 479 (Cal. 1990).
279. *Thornley*, 984 F.3d at 1247.
280. McMahon, *supra* note 25, at 943 n.326.
281. *Id.* at 943; *see also* Hartzog, *supra* note 16, at 101, 103.

good than harm, and hold themselves accountable."[282] It is effective due to its private right of action, wide reach to defendants far outside of Illinois, and the potential for high penalties and attorneys' fees where each individual instance of improper data collection constitutes a separate violation.[283]

The federal courts should not truncate the Illinois legislature's goal of providing essential protections for biometric data through gatekeeping tactics disguised as constitutional restrictions. After *TransUnion*, BIPA plaintiffs only have a fighting chance at successfully clearing the Article III hurdle if they plead with exceptional care. Plaintiffs should seek to emphasize the intent of the Illinois legislature, which clearly sought to protect the right to control one's body and the information that extends from it, like biometrics. The legislature determined that the most effective way to protect people's ability to control information about their body was by creating an individualized right to the necessary safeguards, which thus empowered plaintiffs to vindicate themselves when violated.

282. Jillson, *supra* note 78.

283. McMahon, *supra* note 25, at 943.