Saint Louis University Law Journal

Volume 65
Number 4 *Tradeoffs: Technology, Privacy, and the Law (Summer 2021)*

Article 10

2021

Illinois Biometric Information Privacy Act Litigation in Federal Courts: Evaluating the Standing Doctrine in Privacy Contexts

Michael McMahon

ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT LITIGATION IN FEDERAL COURTS: EVALUATING THE STANDING DOCTRINE IN PRIVACY CONTEXTS

ABSTRACT

Biometric technology, used to identify individuals based on their unchangeable and unique attributes such as fingerprints or facial geometry, has become commonplace in modern life. In Illinois, the use of biometric information by private organizations is regulated by the Illinois Biometric Privacy Act ("BIPA"), which came into effect in 2008 as the nation's first state biometric information privacy statute. BIPA is unique in that it includes a private right of action and provides for recovery of liquidated damages where the statute is violated, which has resulted in plaintiffs bringing steadily increasing numbers of class-action suits under the law. This note examines, in three parts, the current circuit split regarding Article III standing in federal courts that has arisen from BIPA litigation where only procedural BIPA violations are alleged (i.e., where there was a technical violation of the law which purportedly caused no direct harm to the plaintiff). It first explores the history and provisions of BIPA and federal litigation brought under the statute. The note next examines federal jurisdiction over BIPA suits, current Article III jurisprudence, and the history of the circuit split, including how standing has been determined in BIPA suits in the Second, Seventh, and Ninth Circuits. Finally, the note hypothesizes how the Supreme Court might resolve this split in a future ruling, analyzes the impact such a resolution could have, and provides an opinion on the correct resolution.

INTRODUCTION

Biometric technology, used to identify individuals based on their unchangeable and unique attributes (such as fingerprints, facial scans, retinas, etc.), has quickly become commonplace over the last several years as biometrics are incorporated into many popular devices across different areas of our lives. Fingerprint scanners are used for everything from checking in guests at tanning salons and theme parks to timekeeping at many workplaces. Iris recognition—the scanning of an individual's unique iris in their eye for identification—is used by governments in border security and military applications.[1] Most people do not think twice about unlocking their iPhone by quickly glancing their face towards the phone (thus allowing the device to capture a facial scan). Once this biometric information has been collected, analyzed, and identified as belonging to the same person to whom the phone belongs, the phone is unlocked and ready for use—all in the span of a second and without lifting a finger.

Each of these scenarios represent a use of biometric data—the physical and personal characteristics that make each human being unique. Biometric data has been defined as "a digital or analog representation of physical attributes that can be used to uniquely identify us."[2] Biometrics enable digital technologies to recognize and notify us when we appear in photos on social media that we weren't tagged in and are quickly replacing the scanning of a badge as an efficient, foolproof means of clocking in at work. However, what makes biometrics so ideal for identification purposes is the fact that biometric technology analyzes users' unchangeable physical characteristics to determine their identity—meaning that when there is a data breach containing biometric information, the data that has leaked is users' unique physical characteristics; they cannot simply change their password to protect their information.

The Illinois Biometric Privacy Act ("BIPA" or the "Act") has been in effect since 2008 and was the nation's first state statute protecting biometric information.[3] Biometric data is protected, to varying degrees, in state statutes elsewhere: both Texas and Washington also have statutes covering biometric

1. *See, e.g.*, Spencer Ackerman, *U.S. Scans Afghan Inmates for Biometric Database*, WIRED (Aug. 25, 2010, 12:37 PM), https://www.wired.com/2010/08/military-prison-builds-big-afghan-biometric-database/ [https://perma.cc/28S4-ZNAZ]; Ahmad N. Al-Raisi & Ali M. Al-Khouri, *Iris Recognition and the Challenge of Homeland and Border Control Security in UAE*, 25 TELEMATICS & INFORMATICS 117, 124 (2008).

2. *New NIST Biometric Data Standard Adds DNA, Footmarks and Enhanced Fingerprint Descriptions*, NAT'L INST. OF STANDARDS & TECH. (Dec. 6, 2011), https://www.nist.gov/news-events/news/2011/12/new-nist-biometric-data-standard-adds-dna-footmarks-and-enhanced [https://perma.cc/9ME2-R9GF].

3. Rosa M. Tumialàn, et. al., *BIPA Class Actions: The Next Generation of Data Privacy Liability Coverage*, DRI FOR THE DEFENSE 50, 50 (May 2019).

information privacy specifically,[4] while in California, the California Consumer Privacy Act ("CCPA") includes biometric information as a type of personal information subject to the law's protections,[5] and California voters additionally passed Proposition 24, known as the California Privacy Rights Act of 2020 ("CPRA"), in November 2020.[6] The CPRA will, among other changes, designate biometric information processed "for the purpose of uniquely identifying a consumer" as "sensitive personal information",[7] a new category of personal information that provides consumers with additional safeguards.[8] Finally, other states include biometric information protections in their general data security breach notification statutes,[9] and some states have statutes specific to the use of genetic information as well.[10]

Under BIPA, private entities can be liable for significant damage awards for their routine handling of biometric data. The Act's specific provisions are discussed in more detail in Section I.A of this note. BIPA is unique among biometric laws in that it affords a private right of action to individuals, providing that "[a]ny person aggrieved" by a violation of its provisions "shall have a right of action" against an "offending party."[11] Further, the Act provides for recovery

4. Michelle J. Anderson & Jim Halpert, *Washington Becomes the Third State with a Biometric Privacy Law: Five Key Differences*, 1 J. ROBOTICS, A.I. & L. 41, 41 (Jan.–Feb. 2018).

5. Charles N. Insler, *How to Ride the Litigation Rollercoaster Driven by the Biometric Information Privacy Act*, 43 S. ILL. U. L. J. 819, 821 (Summer 2019).

6. Matthew A. Diaz & Kurt R. Hunt, *California Approves the CPRA, a Major Shift in U.S. Privacy Regulation*, NAT'L L. REV. (Nov. 17, 2020), https://www.natlawreview.com/article/california-approves-cpra-major-shift-us-privacy-regulation [https://perma.cc/XY8Q-P49U].

7. *Text of Proposed Laws: California General Election, Tuesday, November 3, 2020*, CALIFORNIA SECRETARY OF STATE 1, 58 (Aug. 10, 2020), https://vig.cdn.sos.ca.gov/2020/general/pdf/topl.pdf [https://perma.cc/W9JG-XMBA].

8. *See* Cynthia Cole et al., *Move Over, CCPA: The California Privacy Rights Act Gets the Spotlight Now*, BLOOMBERG LAW (Nov. 16, 2020, 3:00 AM), https://news.bloomberglaw.com/daily-labor-report/move-over-ccpa-the-california-privacy-rights-act-gets-the-spotlight-now [https://perma.cc/2YB9-LLWT].

9. Connecticut, Iowa, Nebraska, North Carolina, Oregon, Wisconsin, and Wyoming include biometric information in their general data breach statutes. *See* Jason B. Binimow, *Annotation, State Statutes Regulating Collection or Disclosure of Consumer Biometric or Genetic Information*, 41 A.L.R. Fed. 7th Art. 4 (2019). Arkansas and New York have recently added biometric information as well. Natalie Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need to Know in 2020*, LAW.COM (Nov. 15, 2019), https://www.law.com/therecorder/2019/11/15/the-anatomy-of-biometric-laws-what-u-s-companies-need-to-know-in-2020/ [https://perma.cc/8MGY-MZSH].

10. *See, e.g.*, Alaska Genetic Privacy Act, ALASKA STAT. § 18.13.010 (2019) (strictly limiting genetic testing and access to, retention, and disclosure of genetic data without the "informed and written consent" of the individual); NEV. REV. STAT. §§ 629.101–201 (2019) (prohibiting the collection, retention, or disclosure of genetic information without obtaining consent from the individual).

11. 740 ILL. COMP. STAT. 14/20 (2019). This can be compared with other state biometric privacy laws that reserve enforcement to attorneys general: for example, Washington State's

of liquidated damages in the event an entity violates the Act,[12] meaning the issue of who is considered a "person aggrieved" by BIPA violations can have significant financial and remedial consequences for defendants.

This note will discuss the current circuit split regarding Article III standing in federal courts that has arisen from litigation concerning procedural BIPA violations (i.e., where there was a technical violation of the law, which purportedly caused no direct harm) alleged against corporate users of biometrics, including technology services such as photo-sharing websites, social media platforms, video games, and employers. In 2017, the Second Circuit, in an unpublished opinion, dismissed a BIPA claim for lack of standing in *Santana v. Take-Two Interactive Software*.[13] In August 2019, the Ninth Circuit reached the opposite conclusion in *Patel v. Facebook, Inc.*, holding that the procedural violations at issue harmed a concrete interest, giving the plaintiffs standing to sue.[14] By that time, the Seventh Circuit, which covers Illinois, had not ruled on BIPA standing (except in one case applicable only to a narrow subset of transportation-industry employees), though the district courts beneath it had issued conflicting opinions on the matter.[15] This changed in May 2020, when the Seventh Circuit in *Bryant v. Compass Group USA, Inc.* held that certain procedural violations of BIPA constituted a concrete injury sufficient to give standing, while also holding that other procedural violations were not concrete injuries and thus were insufficient to confer standing.[16] The Seventh Circuit further expanded its BIPA jurisprudence in *Fox v. Dakkota Integrated Systems*,[17] where it found Article III standing, and *Thornley v. Clearview AI*, where it did not.[18] The issue of federal standing in BIPA litigation remains unresolved after

biometric privacy statute states that its provisions "may be enforced solely by the attorney general . . . " WASH. REV. CODE § 19.375.030(2) (2019). Similarly, the biometric privacy statute in Texas provides for violators to be subject to a maximum per-violation penalty, stating that "[t]he attorney general may bring an action to recover the civil penalty." TEX. BUS. & COM. CODE ANN. § 503.001(d) (West 2019).

12. 740 ILL. COMP. STAT. 14/20(1)–(2) (2019).

13. 717 F. App'x. 12, 18 (Nov. 21, 2017). While *Santana* is a summary order, meaning it does not have precedential effect in the Second Circuit, splits involving "unpublished order[s]" have garnered attention of the Court before. *See, e.g.*, Lynce v. Mathis, 519 U.S. 433, 436 (1997) (Court granted certiorari "to resolve the conflict" where the Tenth Circuit reached a different conclusion on similar facts than the Eleventh Circuit's earlier unpublished order).

14. 932 F.3d 1264, 1267 (9th Cir. 2019).

15. *See, e.g.*, Rivera v. Google, Inc., 366 F. Supp. 3d 998, 1014 (N.D. Ill. 2018) (dismissing for lack of subject matter jurisdiction "because Plaintiffs have not suffered concrete injuries for Article III purposes"); Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *8 n.5 (N.D. Ill. Sept. 15, 2017) (concluding that "[Plaintiff] has alleged a sufficient injury-in-fact for Article III purposes").

16. Bryant v. Compass Group USA, Inc., 958 F.3d 617, 619, 626 (7th Cir. 2020) (concerning consumer use of vending machines utilizing biometric technology).

17. 980 F.3d 1146, 1156 (7th Cir. 2020).

18. 984 F.3d 1241, 1249 (7th Cir. 2021).

these opinions, and, in the wider context of data privacy litigation, Article III standing to sue in federal court remains a critical issue for plaintiffs in most data privacy causes of action, especially putative class actions.[19]

Section I of this note discusses the history and provisions of the Act, BIPA's place within the wider privacy regulatory framework in the U.S., and federal litigation arising under the statute. Section II examines federal jurisdiction in BIPA suits, the determination of Article III standing in federal courts, the history of the circuit split regarding federal BIPA standing, and how standing has been determined in BIPA litigation in the Second, Seventh, and Ninth Circuits. Section III applies the earlier discussions and analysis to hypothesize how the Supreme Court might resolve this split in a potential future ruling, analyzes the impact such a resolution could have, and provides an opinion on the correct resolution.

I. BACKGROUND

A. BIPA's Applicability and Provisions

BIPA was introduced into the Illinois Senate in February 2008 and passed into law later that year.[20] The Act was designed to address the growth in the use of biometric information in the business and security sectors, the fact that the members of the public were "weary" of such use, the inability of consumers to change their own biometric identifiers, and because the "full ramifications of biometric technology [were] not fully known."[21]

BIPA regulates the use of biometric data in all private businesses, nonprofits, and other associations.[22] It exempts from its coverage public-sector organizations, specifically any "[s]tate or local government agency" or "any court of Illinois, a clerk of the court, or a judge or justice thereof."[23]

BIPA imposes five requirements upon private entities who handle biometric data: notification, consent, ban on profit, ban on disclosure, and storage and security requirements. The alleged violation of any or all of these provisions,

19. CLASS ACTION LITIGATION, 3 E-COMMERCE AND INTERNET LAW 26.15 (Apr. 2020), Westlaw (database updated Apr. 2020).

20. Anna L. Metzger, Comment, *The Litigation Rollercoaster of BIPA: A Comment on the Protection of Individuals from Violations of Biometric Information Privacy*, 50 LOY. U. CHI. L.J. 1051, 1062–63 (2019).

21. 740 ILL. COMP. STAT. 14/5 (2018). It has been noted that "[f]ew outsiders paid attention to negotiations over BIPA," in contrast to attempts to pass data-privacy legislation in the current environment, where "tech companies unleash armies to deflect or shape proposed regulations." Shira Ovide, *The Best Law You've Never Heard Of*, N.Y. TIMES (Feb. 23, 2021), https://www.nytimes.com/2021/02/23/technology/the-best-law-youve-never-heard-of.html [https://perma.cc/TGR6-KRRA].

22. 740 ILL. COMP. STAT. 14/10 (2018).

23. *Id.*

particularly the notification, consent, and disclosure requirements, serves as the harm for which the plaintiff is seeking a remedy in suits brought under BIPA.

The notification provision requires that private entities who possess biometric data must develop and make publicly available a written policy that details how long the entity will retain the biometric data and a schedule for the permanent destruction of biometric data. BIPA requires destruction of biometric data once the initial purpose for collecting the data has been fulfilled or within three years of the individual's last interaction with the private entity, whichever occurs first.[24]

The consent provision consists of three requirements that must be fulfilled for a private entity to be allowed to handle biometric data. First, it must inform the individual in writing that their biometric data is being collected.[25] Second, it must inform the individual in writing of the purpose of the biometric collection and the length for which the biometric data will be collected, stored, and used.[26] Third and finally, it must receive a written release for the biometric collection that is executed by the individual whose biometric data is being collected.[27]

The ban on profit provision prohibits any private entity from selling, leasing, trading, or "otherwise [profiting] from a person's or a customer's biometric [data]."[28] The disclosure ban provision forbids a private entity from the disclosure, redisclosure, or other dissemination of an individual's biometric data except where the data subject has consented to the disclosure or redisclosure, or where the disclosure or redisclosure completes a financial transaction that the data subject has requested or authorized.[29] The Act also allows for disclosure or redisclosure where required by federal, state, or local law or by valid warrant or subpoena.[30]

The storage and security requirements provision requires, first, that private entities use "the reasonable standard of care within the private entity's industry" when storing, transmitting, and protecting from disclosure of biometric data in their possession.[31] Second, it requires private entities—when storing, transmitting, and protecting from disclosure of the biometric data they possess—to use "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."[32]

24. 740 ILL. COMP. STAT. § 14/15(a) (2019).
25. *Id.* § 14/15(b)(1).
26. *Id.* § 14/15(b)(2).
27. *Id.* § 14/15(b)(3).
28. *Id.* § 14/15(c).
29. 740 ILL. COMP. STAT. § 14/15(d)(1)–(2) (2019).
30. *Id.* § 14/15(d)(3)–(4).
31. *Id.* § 14/15(e)(1).
32. *Id.* § 14/15(e)(2).

Though BIPA is an Illinois statute, its reach can extend far beyond Illinois, implicating defendants with no Illinois operations, who may be surprised to find out they are subject to the Act's requirements.[33] While courts have stated that the Act does not apply extraterritorially,[34] to determine whether BIPA litigation can proceed, courts perform a fact-intensive personal jurisdiction analysis to determine whether Illinois courts have jurisdiction over a defendant. Courts have general jurisdiction if the corporate defendant has continuous and systematic affiliations with Illinois to render them essentially at home in the state and specific jurisdiction if there is sufficient affiliation between Illinois and the underlying controversy.[35] Though courts have dismissed BIPA suits for lack of personal jurisdiction due to a defendant's lack of contacts with Illinois,[36] dismissal for lack of personal jurisdiction is a relatively rare occurrence. Most BIPA suits are brought against either an employer with Illinois facilities and/or employees or a consumer-facing company who uses biometrics and sufficiently targets Illinois consumers, both of which are sufficient to establish a court's personal jurisdiction over a defendant.

Recent BIPA jurisprudence on the subject of BIPA's geographic reach serves mostly as a reminder that even entities far away from Illinois should be aware of the law. In *Bray v. Lathem Time Co.*, the court contemplated a suit against a company that made workplace timekeeping systems which utilized biometrics.[37] It dismissed the case because it lacked personal jurisdiction over the defendant, a company based in Georgia with no Illinois operations who only advertised its timekeeping systems to third-party employers, not the plaintiffs.[38] However, in a similar case, *Figueroa v. Kronos Inc.*, the Northern District of Illinois refused to dismiss for lack of personal jurisdiction a case brought against the maker of a different biometric-based timekeeping system, which was utilized by the plaintiffs' employers.[39] The court did not discuss personal jurisdiction, but noted that the defendant sold its systems to "thousands of employers in Illinois" and found that BIPA requires all entities handling biometrics to comply, including both an employer who uses biometric-based timekeeping systems and

33. In fact, commentators have noted that "[t]he extent of BIPA's geographical reach is not yet fully known." Taylor Levesque, et al., *Beyond Borders: COVID-19 Highlights the Potential Widespread Impact of the Illinois Biometric Information Privacy Act ("BIPA")*, LOCKE LORD QUICKSTUDY (May 21, 2020), https://www.lockelord.com/newsandevents/publications/2020/09/beyond-borders-covid19-highlights [https://perma.cc/3UJQ-XQ3R].

34. Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017).

35. *See* McGoveran v. Amazon Web Servs., Inc., No. 3:20-CV-31-NJR, 2020 WL 5602819, at *10–11 (S.D. Ill. Sept. 18, 2020).

36. *See* Bray v. Lathem Time Co., No. 19-3157, 2020 WL 1492742, at *11 (C.D. Ill. Mar. 27, 2020).

37. *Id.* at *1.

38. *Id.* at *12–13.

39. Figueroa v. Kronos Inc., 454 F. Supp. 3d 772, 779, 792 (N.D. Ill. 2020).

the companies who supply those systems.[40] Thus, it would behoove all companies with customers in Illinois to note the potential for liability under BIPA.

BIPA's private right of action, afforded to any individual "aggrieved" under the statute, provides for either liquidated damages of $1,000 or actual damages, whichever is greater, per negligent violation, and for liquidated damages of $5,000 or actual damages, whichever is greater, per intentional or reckless violation.[41] However, "BIPA does not define 'intentionally' or 'recklessly.'"[42] Courts use the Illinois common law definitions of these terms.[43] While many suits claim reckless or intentional violations, not a single BIPA case has made it to trial,[44] so there is limited jurisprudence to illustrate the difference between negligent and intentional or reckless BIPA violations.[45] Recent BIPA decisions clarify that mere conclusory statements, where plaintiffs allege intentional and reckless BIPA violations, are insufficient to overcome a motion to dismiss,[46] while on the other hand, defendants who have "made no effort to comply with BIPA" may be committing reckless or intentional violations of the Act if they have not made an attempt to comply.[47]

The stakes for companies who use biometrics in their products and services are quite high. Not only can there be penalties for each *user* for the improper collection of their biometric information, but courts have interpreted BIPA to allow for penalties for *each specific instance* of improper biometric collection.[48]

40. *Id.* at 779, 783.

41. 740 ILL. COMP. STAT. § 14/20 (2019).

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

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

44. As of January 2020. Allison Grande & Ben Kochman, *BIPA Bares Its Teeth in Facebook Biometric Privacy Deal*, LAW360 (Jan. 30, 2020, 10:39 PM), https://www.law360.com/articles/1239383/ [https://perma.cc/75X4-SUBX].

45. *See* Celeste Bott, *Breaking Down Illinois' Biometric Privacy Litigation Boom*, LAW360 (Apr. 27, 2020, 8:15 PM), https://www.law360.com/articles/1252596/breaking-down-illinois-biometric-privacy-litigation-boom [https://perma.cc/8GHZ-AVHY]. ("[T]wo of the major [BIPA] defenses have yet to be tested at all. One of those defenses is what it means under BIPA for a defendant to be negligent or reckless for damages purposes.").

46. *Rogers*, 409 F. Supp. 3d at 619.

47. Peatry v. Bimbo Bakeries USA, Inc., No. 19 C 2942, 2020 WL 919202, at *6 (N.D. Ill. Feb. 26, 2020).

48. *See* Cothron v. White Castle System, Inc., 477 F. Supp. 3d 723, 732 (N.D. Ill. 2020). Whether this interpretation will remain good law, though, remains in question—the defendant has appealed to the Seventh Circuit. *See* Lauraann Wood, *White Castle Urges 7th Cir. To Limit BIPA Claim Accrual*, LAW360 (Mar. 30, 2021, 5:05 PM), https://www.law360.com/articles/1370291 [https://perma.cc/P8SK-AUT2].

This can result in damages that can quickly become, in the words of one BIPA defendant, "crippling."[49]

B. BIPA's Role in the U.S. Data Privacy Regulatory Scheme

BIPA occupies a unique place in the current data protections available to American consumers in Illinois. Across the Atlantic, there is comprehensive privacy regulation in Europe via the General Data Protection Regulation ("GDPR") which provides European Union citizens with, among other things, the ability to monitor how companies use their data and the power to direct companies in possession of their data to destroy it.[50] Biometric information is included in the GDPR as "sensitive personal data" which provides additional protections.[51] In the United States, there is little in the way of any substantive data privacy controls outside of California. Washington and Texas also have statutes concerning the privacy of biometric information, but individuals are not able to enforce these statutes via private actions like they are with BIPA in Illinois; only the states' attorneys general may enforce these biometric privacy laws.[52] While these laws are similar to BIPA, there are important differences. Washington's law, for example, does not apply to employers who use employees' biometrics in their timekeeping systems.[53] Despite the similarities, the lack of private right of action has led commentators to state that "the Washington and Texas laws 'will likely be a footnote'"[54] and ultimately,

49. *Cothron*, 477 F. Supp. 3d at 733.

50. GDPR states that processing the data of natural persons is only lawful in a selected set of circumstances, such as receiving consent of the data subject. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 On the Protection of Natural Persons with Regard to the Processing of Personal Data and On the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) art. 6 [hereinafter GDPR]. Consumers may request a copy of their data and have the right to rectify inaccuracies in their personal data held by third parties as well as to request the deletion of their data. *Id.* at arts. 15–17.

51. The GDPR prohibits the processing of biometric information without the explicit consent of the data subject or other limited exceptions. *Id.* at art. 9.

52. *See* TEX. BUS. & COM. CODE ANN. § 503.001(d) (2019); WASH. REV. CODE § 19.375.030(2) (2020).

53. Philip L. Gordon & Kwabena A. Appenteng, *Dear Littler: What Does Our Company Need To Do Before We Begin Using Biometric Timeclocks?*, LITTLER (Dec. 6, 2017), https://www.littler.com/publication-press/publication/dear-littler-what-does-our-company-need-do-we-begin-using-biometric [https://perma.cc/ES3Z-KUBD].

54. Paul Shukovsky, *Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin*, Bloomberg Law (July 18, 2017, 7:26 AM), https://www.bloomberglaw.com/product/blaw/bloomberglawnews/privacy-and-data-security/X8MBJH0C000000 [https://perma.cc/3ZPY-Y5UA].

because of BIPA's private right of action, it has been the focus of most biometric privacy litigation.[55]

Since January of 2020, California consumers have been given similar powers to the GDPR under California's CCPA.[56] The CCPA considers biometric data as a category of personal data subject to the law's protections,[57] and the recently-passed CPRA, which will take effect in 2023, will place biometric data into a new "sensitive personal information" category with additional safeguards.[58] While the CCPA grants California consumers many new rights to control how private entities use their personal data, enforcement is currently out of the consumer's hands (for the most part). Consumers may only sue when their nonencrypted and nonredacted personal information is accessed by unauthorized third parties as a result of a business's failure to implement and maintain reasonable security.[59] Other than data breaches, enforcement is left to the state attorney general.[60] The CPRA, however, creates additional enforcement mechanisms in addition to those found in the CCPA. It establishes the California Privacy Protection Agency, a state agency with the sole purpose of regulating consumer data privacy that replaces the California attorney general as the chief enforcer of the state's privacy laws.[61] It also expands the private right of action available to individuals.[62]

Consumers in the rest of the country are left with few means to control the use of their data. There are data breach regulations in most states, but these statutes only come into play once data has been disclosed to unauthorized

55. Stephanie Sheridan & Meegan Brooks, *Avoid Getting a Plaintiff's Fingerprint Pointed at You*, LAW360 (Feb. 28, 2018, 1:27 PM), https://plus.lexis.com/api/permalink/490caa85-4d5c-40cc-bc9e-e46e5d60ea3b/?context=1530671 [https://perma.cc/2KXV-FK8K].

56. The CCPA grants consumers the right to opt-out of the sale of their personal information to third parties and requires businesses to notify consumers of the potential sale of their data and their right to opt out. CAL. CIV. CODE §§ 1798.120(a)-(b) (2020); Consumers may request a copy of their information that is held by businesses. *Id.* § 1798.110(a); Consumers also have the right to request that businesses delete their personal information. *Id.* § 1798.105(a); CCPA applies to companies with revenue greater than twenty-five million dollars and those that buy, sell, or share the data of 50,000 or more consumers. *Id.* § 1798.140(c)(1). The International Association of Privacy Professionals estimated that the law will apply to over 500,000 American businesses. Rita Heimes & Sam Pfeifle, *New California Privacy Law to Affect More Than Half a Million US Companies*, INT'L ASS'N OF PRIV. PROS. (July 2, 2018), https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/ [https://perma.cc/E3U7-VAPW].

57. CAL. CIV. CODE § 1798.140(o)(1)(E) (2020).

58. Diaz & Hunt, *supra* note 6.

59. CAL. CIV. CODE § 1798.150(a)(1) (2020).

60. *Id.* § 1798.155(b).

61. Diaz & Hunt, *supra* note 6.

62. Caitlin Fennessy, *CPRA's Top-10 Impactful Provisions*, INT'L ASS'N OF PRIV. PROS. (May 12, 2020), https://iapp.org/news/a/cpra-top-10-impactful-provisions/ [https://perma.cc/Q8KR-NH33].

parties.[63] Breach statutes do little to provide consumers any control over their data—in fact, they may result in consumers only finding out that a company possessed their data in the first place upon being notified of a data breach affecting that company.[64] Federal legislation regarding data and information privacy is relatively scant and most federal information statutes are concerned with promoting the efficient flow of information and regulating specific types of data or sectors of businesses such as healthcare information or financial institutions.[65] Non-sector-specific privacy enforcement may be brought by the Federal Trade Commission ("FTC") under Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or effecting commerce.[66]

63. *See, e.g.*, MO. REV. STAT. § 407.1500 (2019) (requiring owners or licensors of personal information to "provide notice to the affected consumer that there has been a breach of security," which is defined as "unauthorized access to and unauthorized acquisition of personal information"); N.Y. GEN. BUS. LAW § 899-aa (2019) (requiring personal data owners or licensors to "disclose any breach . . . to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization"); TEX. BUS. & COM. CODE ANN. § 521.053 (2019) (requiring data owners or licensors of personal data to disclose breaches to "any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an authorized person").

64. For example, in 2017, a travel services company, Sabre Corporation, was subject to a data breach, which included consumer payment information, in its SynXis reservation system, a software product used to manage reservations at over 36,000 hotel properties. Jamie Biesiada, *Sabre Completes Investigation into Data Breach of Hotel Res System*, TRAVEL WEEKLY (July 6, 2017), https://www.travelweekly.com/Travel-News/Travel-Technology/Sabre-completes-investigation-into-data-breach-of-hotel-res-system [https://perma.cc/C2LE-SHHG]. Consumers who had made reservations at affected hotels likely would have no idea their data was held by Sabre.

65. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d-2–1320d-9 (2018) (regulating healthcare information); Gramm Leach Bliley Act, 15 U.S.C. § 6801 (2018) (regulating data held by financial institutions); Children's Online Privacy Protection Act, 15 U.S.C. § 6502 (2018) (regulating children's information); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2018) (regulating students' information); Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2018) (regulating information found in consumer and credit reports); FCC Customer Proprietary Network Information Breach Rule, 47 C.F.R. § 64.2011 (2017) (notification requirements applicable to telecommunications carriers when information about consumer telephone calls are breached); Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 30, app. B (2014) (requiring notification of security breaches "when warranted" to customers of financial). Many of these federal statutes were enacted before it was common for consumers to use the Internet in a personal capacity. Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J. L. & TECH. 1, 17 (2018).

66. 15 U.S.C. § 45. The FTC levied its first enforcement action based on the misuse of facial recognition technology in 2021, when it reached a proposed settlement with photo app developer Everalbum Inc. *See* Decision and Order, In re Everalbum, Inc., File No. 192-3172 (F.T.C. Jan. 11, 2021), 2021 WL 118895. This was seen as "an unequivocal warning that the FTC will make policing facial recognition technology a priority for the foreseeable future." David J. Oberly, *FTC's First Settlement on Facial Recognition Technology Yields Lessons*, BLOOMBERG LAW (Feb. 18,

Given this state of data privacy regulation in the United States, BIPA is quite unique, and while the history of litigation under the statute is quite brief, it should be viewed as a tool that individuals—at least those who reside in and are citizens of the state of Illinois—can use to protect their privacy and bring about change in the use of biometric information by private companies.[67]

C. BIPA Litigation

BIPA litigation began around 2015,[68] and since then, plaintiffs have brought over 300 suits against companies in a variety of industries.[69] Much of the litigation falls into two groups: employment cases and consumer-technology cases. In employment cases, claims are based on violations of BIPA involving employer use of employee's biometric information and/or identifiers—usually these cases involve time-keeping methods which require employee biometrics, such as using fingerprints to clock in and out of shifts.[70] Consumer-technology

2021, 3:01 AM), https://news.bloomberglaw.com/business-and-practice/ftcs-first-settlement-on-facial-recognition-technology-yields-lessons [https://perma.cc/7ENG-MPTF].

67. Illinois lawyers have noted, in the wake of large settlements in class actions brought under the Act, that "'BIPA not only has teeth, but that those teeth are extremely sharp.'" Grande & Kochman, *supra* note 44. Legal commentators state that "BIPA's private cause of action has meaningfully shaped the practices of companies who deploy biometrics." Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS 96, 97 (Amba Kak ed., 2020), https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf [https://perma.cc/HH5V-YUD6]. One instance of the changes in private companies' behavior brought about by BIPA can be seen in the May 2020 decision by Clearview AI, a facial recognition technology provider, to end all its service contracts with non-law enforcement entities in the hopes of avoiding BIPA damages. *Id.* at 96. Additionally, Clearview stated that it was taking measures to prevent its technology from collecting data from Illinois residents. Nick Statt, *Clearview AI to Stop Selling Controversial Facial Recognition App to Private Companies*, THE VERGE (May 7, 2020, 8:29 PM), https://www.theverge.com/2020/5/7/21251387/clearview-ai-law-enforcement-police-facial-recognition-illinois-privacy-law [https://perma.cc/8TWZ-UVXD]. Despite these (seemingly belated) actions taken to avoid BIPA compliance, Clearview found itself the defendant in several BIPA suits, one of which wound up before the Seventh Circuit. *See* discussion *infra* Section II.D.6.

68. In 2015, the U.S. District Court for the Northern District of Illinois stated that it was "unaware of any judicial interpretation of [BIPA]." Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

69. Gerald L. Maatman, Jr. et al., *Biometric Privacy Class Actions by The Numbers: Analyzing Illinois' Hottest Class Action Trend*, WORKPLACE CLASS ACTION BLOG (June 28, 2019), https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/ [https://perma.cc/DZ5Z-YZVG].

70. *See, e.g.*, Dixon v. Washington & Jane Smith Cmty–Beverly, No. 17 C 8033, 2018 WL 2445292, at *1 (N.D. Ill. May 31, 2018) ("[Plaintiff] asserts claims for . . . violation of Illinois's Biometric Information Privacy Act (BIPA) arising from [defendant's] requirement that its employees clock in and out of work by scanning their fingerprints onto a biometric timekeeping device . . . "); Colon v. Dynacast, LLC, No. 19-cv-4561, 2019 WL 5536834, at *1 (N.D. Ill. Oct. 17, 2019) ("[The plaintiff] filed this putative class action complaint against her former employer

cases involve providers of consumer services, often technology- or media-related services such as video games, social media platforms, and photo-sharing services, but also a number of other services, such as vending machines and tanning salons, who use the biometric information and/or identifiers of their users.[71]

Beyond standing, companies have taken a number of approaches to defend against BIPA claims. In cases involving out-of-state defendants, extraterritoriality defenses may be used.[72] In Illinois, state statutes do not apply extraterritorially unless expressly intended to by the legislature—and there is no sign that this is the case for the Act.[73] Thus, if the Act does not apply extraterritorially, the asserted violations must have taken place in Illinois for plaintiffs to be victorious and violations occurring to Illinois residents outside of Illinois, therefore, would not constitute violations of the Act.[74] Under Illinois law, "there is no single formula or bright-line test for determining whether a transaction occurs within [the] state."[75] Given the digital nature of many BIPA claims, the fact that many defendants are not based in Illinois and the fact that alleged violations may have occurred on remote servers or in the cloud may present an issue for some BIPA actions.[76] However, this defense has not been very successful in BIPA claims brought by consumers, because federal courts have generally found sufficient connections to Illinois meaning BIPA is not being applied extraterritorially.[77] Courts have also noted the lack of "non-residents suing under Illinois law, which is the paradigmatic situation for the presumption against the extraterritorial application of local law."[78]

. . . [who] used so-called biometric data to provide authentication for its time-card system."); Aguilar v. Rexnord LLC, No. 17 CV 9019, 2018 WL 3239715, at *1 (N.D. Ill. July 3, 2018) ("While [the plaintiff] was an employee [of the defendant], [the defendant] implemented a time clock system that used employees' fingerprints to track when employees began and ended their workdays.").

71. *See, e.g.*, *Norberg*, 152 F. Supp. 3d at 1105 ("Defendants operate a number of websites that provide digital photo storage, sharing, and photo prints and novelty gifts . . . "). This note explores several of these types of cases in Section II.

72. *See, e.g.*, Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1100-01 (N.D. Ill. 2017).

73. *Id.* at 1100.

74. *See id.*

75. *Id.* at 1100–01 (quoting Avery v. State Farm Mut. Auto. Ins. Co., 835 N.E.2d 801, 854 (Ill. 2005)).

76. *See* Insler, *supra* note 5, at 822.

77. *See Rivera*, 238 F. Supp. 3d at 1101–02 (noting that the fact that the plaintiffs were Illinois residents, the photographs at issue were taken in Illinois, and were uploaded to the cloud from an Illinois IP address, ultimately weighed in favor of a holding that the alleged violations primarily occurred in Illinois); Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *6 (N.D. Ill. Sept. 15, 2017) (noting that the photo at issue was uploaded to the defendant's website from a device physically located in Illinois and via an Illinois IP address, and that "it [was] unclear" where the actual scan of facial geometry took place and where that scan was stored).

78. In re Facebook Biometric Info. Priv. Litig., 326 F.R.D. 535, 547 (N.D. Cal. 2018).

A related defense involves the dormant commerce clause of the U.S. Constitution, which limits the ability of states to discriminate or burden interstate commerce.[79] In *Monroy v. Shutterfly, Inc.*, a case involving technical violations of BIPA provisions in a social-media photo-tagging context, the defendant argued that the application of BIPA would effectively regulate its conduct outside of Illinois, ultimately "[projecting] . . . one state regulatory regime into the jurisdiction of another State."[80] The District Court for the Northern District of Illinois rejected this argument, stating that "[a]pplying BIPA in this case would not entail any regulation of [the defendant's] gathering and storage of biometric data obtained outside of Illinois" and noted that while the Act does "[require the defendant] to comply with certain regulations if it wishes to operate in Illinois," it does not "[control the defendant's] conduct in other states."[81] Other courts adjudicating other BIPA claims have also rejected this defense.[82]

Another interesting defense arises from the curious wording of the statute: in the definition of "biometric identifier," the Act states that "biometric identifiers do not include . . . photographs."[83] The Act then defines "[b]iometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[84] Thus, it would appear that faceprints derived from photos, which are often the biometric information at issue in social-media BIPA claims, are not considered biometric information under the law and thus not subject to its protections. This has had varying levels of success in federal courts. The District Court for the Northern District of California rejected this argument, finding that the placement in the statute of the photograph exclusion as meaning to only exclude *paper*—not digital—photographs.[85] The District Court for the Northern District of Illinois held that the statute's drafters did intend to exclude all biometric data derived from *any* type of photograph, digital or paper.[86] It also

79. *Monroy*, 2017 WL 4099846, at *7.

80. *Id.*

81. *Id.*

82. Defendant Google raised this defense in *Rivera*, but the court held that it was unable to determine whether BIPA was being used in the case to control commercial conduct wholly outside Illinois because it needed "a better factual understanding of what is happening in the Google Photos face-scan process." Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1103–04 (N.D. Ill. 2017). Facebook raised this defense as well in an earlier stage of the *Patel* litigation, but the district court flatly rejected this argument, noting that "[the] lawsuit is under an Illinois state statute on behalf of Illinois residents who used Facebook in Illinois." In re Facebook Biometric Info. Priv. Litig., No. 3:15-cv-03747-JD, 2018 WL 2197546, at *4 (N.D. Cal. May 14, 2018).

83. 740 ILL. COMP. STAT. 14/10 (2018).

84. *Id.*

85. In re Facebook Biometric Info. Priv. Litig., 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016).

86. Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *3 (N.D. Ill. Sept. 15, 2017).

found an open question of whether data obtained from a digital photograph may constitute a "biometric identifier" under the Act.[87]

The Article III standing issue, however, is the issue on which the *Patel*, *Santana*, *Bryant*, *Fox*, and *Thornley* courts differ and which this note explores. This topic is important in the context of data privacy, as the ability to demonstrate sufficient harm to establish Article III standing has been a major impediment to plaintiffs in data-privacy suits; scholars emphasize that most data breach cases brought in federal courts "have not turned on whether the defendants were at fault" but instead "have been bogged down with the issue of harm."[88]

II. ARTICLE III STANDING & THE BIPA CIRCUIT SPLIT

A. Standing

Questions of plaintiffs' Article III standing are frequently raised by defendants in BIPA claims in order to secure dismissal for lack of subject matter jurisdiction.[89] To establish standing under Article III of the Constitution, "the plaintiff must have suffered an 'injury in fact'—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) 'actual or imminent, not "conjectural" or "hypothetical."'"[90] The Supreme Court instructs that a plaintiff does not "automatically [satisfy] the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[91] As the Ninth Circuit explained, "it is not enough for a plaintiff to allege that a defendant has violated a right created by a statute; [courts] must still ascertain whether the plaintiff suffered a concrete injury-in-fact due to the violation."[92] Thus, for BIPA litigation, standing defenses are most important in the cases in which the alleged violations are purely technical or procedural violations of the statute—i.e., failures to follow the exact instructions provided by the Act— because in these contexts, courts must not only analyze the alleged statutory violation, but also determine whether the plaintiff suffered a concrete injury sufficient to grant standing to sue.

In Illinois state courts, the issue of standing to sue for purely procedural violations of BIPA was resolved by the Illinois Supreme Court's 2019 decision

87. *Id.*

88. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739 (2018). *See also* E-COMMERCE AND INTERNET LAW, *supra* note 19 ("A number data of [sic] privacy putative class action suits and claims have been dismissed for lack of standing . . . Even in security breach cases, standing may be an issue . . . ").

89. Insler, *supra* note 5, at 823.

90. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (citation omitted) (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)).

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

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

in *Rosenbach v. Six Flags Entertainment Corp.*[93] The court stated 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," meaning that "such a person . . . would clearly be 'aggrieved' within the meaning of [BIPA]."[94] The court went on to clarify that "[n]o additional consequences need be pleaded or proved" and that "[t]he violation [of the provisions of BIPA], in itself, is sufficient to support the individual's or customer's statutory cause of action."[95] This ruling settled the matter of whether purely procedural or technical violations of BIPA constitute concrete injuries allowing suits to be brought under the Act in state courts. However, this issue has yet to be resolved in federal courts, where much BIPA litigation occurs;[96] oftentimes, plaintiffs will file suit in state court (where standing is not an issue) only for the case to be removed to federal court by defendants, who seem to have a clear preference for federal court.[97]

Article III of the U.S. Constitution limits the jurisdiction of federal courts by requiring them to hear only actual cases or controversies.[98] This jurisdictional limitation creates the hurdle of Article III standing that suits must clear before proceeding: standing "is the threshold question in every federal case, determining the power of the court to entertain the suit."[99] The Supreme Court's jurisprudence instructs that the constitutional requirement of standing consists of three elements: (1) an actual injury in fact suffered by the plaintiff, "(2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision."[100] To meet the "injury-in-fact" requirement, a plaintiff must suffer "an invasion of a legally protected interest" which must be (a) "concrete and particularized" and (b) "actual or

93. 129 N.E.3d 1197 (Ill. 2019).

94. *Id.* at 1206.

95. *Id.*

96. In *Bryant*, the Seventh Circuit noted that "[h]elpful though *Rosenbach* may be, . . . we cannot uncritically assume perfect overlap between the question before the state court and the one before us" because "standing requirements in Illinois courts are more lenient than those imposed by Article III." Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 622 (7th Cir. 2020) (citing Greer v. Illinois Hous. Dev. Auth., 524 N.E.2d 561, 574 (Ill. 1988)).

97. Jennifer Marsh, *ANALYSIS: 7th Circuit's BIPA Rulings Provide State Court Roadmap*, BLOOMBERG LAW (Feb. 18, 2021, 10:46 AM), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-7th-circuits-bipa-rulings-provide-state-court-roadmap [https://perma.cc/TF6W-HNKS] (finding, in a review of Illinois federal district court dockets from November 2020 through January 2021, that only 12 BIPA complaints were originally filed in federal court, but at least 36 were removed to federal court from state courts).

98. U.S. CONST. art. 3, § 2, cl. 1.

99. Mahon v. Ticor Title Ins. Co., 683 F.3d 59, 62 (2d Cir. 2012) (quoting Warth v. Seldin, 422 U.S. 490, 498 (1975)).

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

imminent, not 'conjectural' or 'hypothetical.'"[101] If the alleged injury is imminent, it must be "*certainly impending* to constitute injury in fact."[102] The alleged imminent injury cannot consist merely of "[a]llegations of *possible* future injury."[103] Finally, the Supreme Court has instructed that a plaintiff does 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."[104]

In *Spokeo*, the Court elaborated on the concreteness requirement that is necessary to demonstrate injury-in-fact when bringing suit for statutory violations. In that case, the Court reviewed the Ninth Circuit's decision to reverse the district court's dismissal of the plaintiff's action against defendant Spokeo under the Fair Credit Reporting Act of 1970 ("FCRA").[105] Spokeo operated a website where users could search for other individuals by name, e-mail, or phone number and gather information, including address, marital status, approximate age, occupation, finances, hobbies, and other types of information about that individual from a wide variety of databases that were indexed and searched by Spokeo.[106] The plaintiff alleged that Spokeo qualified as a "consumer reporting agency" as defined by the FCRA, and was thus required to follow reasonable procedures to ensure the maximum accuracy of consumer reports, notify providers and users of consumer information of their responsibilities under the FCRA, limit the provision of consumer reports for employment purposes, and post toll-free phone numbers where consumers can request reports.[107] The FCRA further provides that agencies who fail to follow its requirements are liable to individuals for actual damages or statutory damages, ranging from $100 to $1,000 per violation, and attorney's fees.[108] The plaintiff brought suit under the FCRA, alleging that a search for him using Spokeo's website generated inaccurate information.[109]

In its discussion of the concreteness requirement, the Court noted that "concrete" harms are not always "tangible," and affirmed the importance of the legislature in identifying, via statute, intangible harms that meet Article III requirements.[110] The Court reasoned that the FCRA protected against the concrete harm of false information by attempting to "curb the dissemination of

101. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)).

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

103. *Id.*

104. *Spokeo*, 136 S. Ct. at 1549.

105. *Id.* at 1544.

106. *Id.* at 1546.

107. *Id.* at 1545–46.

108. *Id.* at 1545.

109. *Spokeo*, 136 S. Ct. at 1546.

110. *Id.* at 1549.

[false information] by adopting procedures designed to decrease that risk."[111] However, the Court stated that "a plaintiff [does not] automatically satisf[y] the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right," emphasizing that "Article III standing requires a concrete injury even in the context of a statutory violation."[112] Thus, the statutory right to sue is not always enough under the Constitution: even if a statute authorizes private lawsuits in the event the statute is violated, and even if there has actually been a violation of the statute, there must *still* be a concrete injury to have jurisdiction in federal court. While the Court instructed that "the risk of real harm" can satisfy the requirement of concreteness in the right instances, it concluded that there must be *some* harm or material risk of harm *beyond* a "bare procedural violation" of a statute to satisfy Article III's requirements.[113] The case was remanded back to the Ninth Circuit to perform a proper analysis of the concreteness of the injuries alleged by the claim.[114]

On remand, the Ninth Circuit undertook a concreteness analysis and concluded that there were allegations of injuries sufficiently concrete to confer standing to sue.[115] In this analysis, the court first asked whether the statutory provision at issue was established to protect a concrete interest, as opposed to purely procedural rights, and, second, whether the specific procedural violations alleged in the case actually harmed or presented a material risk of harm to those interests.[116] The court determined that the protections given by the FCRA were "'real,' rather than purely legal creations," citing the legislative record discussing how inaccuracies in consumer reports could harm consumers, the importance of consumer reports in modern life (noting their use in employment decisions, loan applications, and home purchases), as well as the fact that the Supreme Court's ruling in *Spokeo* did assume that false information in consumer reports does at least have the potential to constitute a concrete harm.[117]

On the second part of the analysis, whether the specific procedural violations at hand actually harmed or presented a material risk of harm, the court held that there was a material risk of harm.[118] The court noted the importance of the "examination of the *nature* of the specific alleged reporting inaccuracies to ensure that they raise a real risk of harm to the concrete interests that FCRA protects."[119] Citing the Supreme Court's guidance that "it cannot be the case that

111. *Id.* at 1550.
112. *Id.* at 1549.
113. *Id.* at 1549–50.
114. *Spokeo*, 136 S.Ct. at 1550.
115. Robins v. Spokeo, Inc., 867 F.3d 1108, 1118 (9th Cir. 2017).
116. *Id.* at 1113.
117. *Id.* at 1114 (citing *Spokeo*, 136 S. Ct. at 1550).
118. *Id.* at 1116.
119. *Id.*

every trivial or meaningless inaccuracy" presents a real risk of harm, the court held that the specific procedural violations at issue—the publication by Spokeo on the Internet of multiple inaccuracies about the plaintiff, including his wealth level, marital status, age range, field of employment, and educational status—constituted a real risk of harm to the concrete interests protected by the FCRA.[120] Thus, the court concluded, there was standing to sue.[121]

The Supreme Court's guidance from *Spokeo* on what constitutes a concrete injury, and the framework for the proper analysis of concreteness, informs much of the subsequent BIPA litigation in federal courts.

B. Federal Jurisdiction in BIPA Class-Action Suits

Generally, federal BIPA cases are large class action suits brought by Illinois plaintiffs against out-of-state companies who use biometrics.[122] This provides the diversity required for the federal courts to have jurisdiction under 28 U.S.C. § 1332; however, the diversity jurisdiction statute also requires the matter in controversy be in excess of $75,000 exclusive of interest and costs.[123] Although this depends on the number of times the defendant made unauthorized collections of the plaintiff's biometric information (committed a BIPA violation)—given that BIPA only provides for liquidated damages of $1,000 per negligent violation and $5,000 per intentional or reckless violation—there would need to be 75 instances of negligent violations at $1,000 each, or 15 instances of intentional or reckless violations at $5,000 each, for an individual plaintiff's case to meet the amount-in-controversy requirement necessary for federal jurisdiction under section 1332.

Thus, most BIPA suits arrive in federal court based on diversity jurisdiction and the Class Action Fairness Act ("CAFA").[124] CAFA calls for minimal

120. *Robins*, 867 F.3d at 1116–17.

121. *Id.* at 1118.

122. For example, in *Patel v. Facebook*, the plaintiffs were residents and citizens of Illinois, while the defendant, Facebook, was a Delaware corporation with its headquarters and principal place of business in California. *See* Consolidated Class Action Complaint, Licata v. Facebook, Inc., No. 3:15-cv-03747-JD (N.D. Cal. Aug. 28, 2015), 2015 WL 13691679. Similarly, in *Rivera v. Google*, the representative plaintiff was a resident and citizen of Illinois and the defendant, Google, was a Delaware corporation with its headquarters in California. *See* First Amended Class Action Complaint, Weiss v. Google Inc., No. 1:16-cv-02714 (N.D. Ill. May 27, 2016), 2016 WL 3438680. In *Santana v. Take-Two Interactive Software*, the defendant Take-Two was a Delaware corporation with its headquarters and principal place of business in New York, while the plaintiffs were residents and citizens of Illinois. *See* Second Amended Class Action Complaint, Vigil v. Take-Two Interactive Software, Inc., No. 1:15-cv-08211-JGK (S.D.N.Y. July 15, 2016), 2016 WL 3965052.

123. *See* 28 U.S.C. § 1332(a) (2018).

124. *Id.* § 1332(d); *see, e.g.*, Rogers v. CSX Intermodal Terminals, Inc., 409 F. Supp. 3d 612, 614 (N.D. Ill 2019) (stating that the case was initially filed in the Circuit Court of Cook County and that "[defendant] then removed the case to [federal district] court based on diversity jurisdiction and the Class Action Fairness Act").

diversity, requiring only any member of a class of plaintiffs to be a citizen of a state different from any defendant,[125] and requires the matter in controversy to exceed the sum or value of $5,000,000, exclusive of interest and costs.[126] Under CAFA, the claims of each individual class member are aggregated to determine whether the matter in controversy exceeds the sum of value of five million dollars.[127] To show whether removal to federal court is proper, a defendant must only convince the federal court that, by the preponderance of the evidence, the amount in controversy meets the five million dollar threshold.[128] Once removed to federal court, cases are only remanded back to state court if it can be demonstrated that it is *impossible* for the plaintiff to recover at least the amount of the amount-in-controversy requirement.[129]

By proposing a plaintiff class of Illinois residents who are users of large technology services such as Google or Facebook, or are employees of large employers who use biometric information in the workplace, the liquidated damages BIPA provides for quickly reach the five million dollar amount-in-controversy minimum—allowing for federal jurisdiction under CAFA.[130] The District Court for the Northern District of California, in its order certifying a class of plaintiffs suing Facebook for BIPA damages, noted that the Act's liquidated damages "are not enough to incentivize individual plaintiffs given the high costs of pursuing discovery on [the defendant] and . . . willingness [of the defendant, a large multinational corporation,] to litigate."[131] Thus, CAFA provides the basis for federal jurisdiction in most federal BIPA litigation.

C. A Brief History of the Circuit Split

Over the last several years, a conflict among federal courts has arisen regarding what constitutes standing to sue for BIPA litigants. In *Patel*, a 2019 Ninth Circuit decision, the plaintiff alleged BIPA violations based on Facebook's photo-tagging feature, which scans photos uploaded to Facebook for faces of other Facebook users, and suggests the uploader to "tag" those users

125. 28 U.S.C. § 1332(d)(2)(A) (2018).

126. *Id.* § 1332(d)(2).

127. *Id.* § 1332(d)(6).

128. *Id.* § 1446(c)(2)(B).

129. Spivey v. Vertrue, Inc., 528 F.3d 982, 986 (7th Cir. 2008) ("Once the proponent of federal jurisdiction has explained plausibly how much the stakes exceed five million dollars, then the case belongs in federal court unless it is legally impossible for the plaintiff to recover that much.").

130. *See, e.g.*, Peatry v. Bimbo Bakeries USA, Inc., 393 F. Supp. 3d 766, 769 (N.D. Ill. 2019) ("[Defendant] claims that the Court has jurisdiction under CAFA, with a class of at least 300 members needing to only scan their fingerprints four times each to exceed CAFA's five-million-dollar amount in controversy requirement").

131. In re Facebook Biometric Information Privacy Litigation, 326 F.R.D. 535, 548 (N.D. Cal. 2018).

identified in the photo.[132] Ultimately, the court rejected Facebook's claim that the plaintiffs failed to allege a concrete injury-in-fact.[133]

This conflicts with the Second Circuit's ruling in *Santana v. Take-Two Software, Inc.*, an unpublished 2017 case in which the court reviewed the district court's dismissal for lack of Article III standing.[134] The Second Circuit upheld the district court's dismissal, finding that the plaintiffs "failed to show a 'real risk of harm' sufficient to confer an injury-in-fact."[135]

At the time of the *Patel* ruling, the Seventh Circuit had not weighed in on BIPA standing in any cases involving consumer services. It had, however, found Article III standing in an employment context in *Miller v. Southwest Airlines Co*.[136] On the other hand, lower courts beneath the Seventh Circuit had, for the most part, rejected finding standing for procedural BIPA violations, absent some further harm, in both employment and consumer cases.[137] The Seventh Circuit ruled on BIPA standing in a consumer context in *Bryant v. Compass Group USA, Inc.*, which involved vending machines which used fingerprint scanning to identify the individual making the purchase for billing purposes.[138] Here, the Seventh Circuit muddied the waters even further, agreeing with the Ninth Circuit that procedural violations of BIPA's notification and consent requirements[139] were sufficient to confer standing,[140] while a violation of the requirement to disclose a deletion policy and retention schedule[141] was insufficient.[142] Following *Bryant*, the Seventh Circuit again ruled on BIPA in *Fox v. Dakkota Integrated Systems*, a case brought against an employer by an employee where

132. Patel v. Facebook, Inc., 932 F.3d 1264, 1267–68 (9th Cir. 2019).

133. *Id.* at 1267.

134. 717 F. App'x. 12, 13–14 (2d Cir. 2017).

135. *Id.* at 17 (quoting Spokeo Inc., v. Robins, 136 S. Ct. 1540, 1549 (2016)).

136. 926 F.3d 898 (7th Cir. 2019)). This note explores this decision further in Section II.D.3.

137. *See, e.g.*, Hunter v. Automated Health Sys., Inc., 2020 WL 833180 at *1–2 (N.D. Ill. Feb. 20, 2020) (Employee's suit against employer alleging BIPA violations in employer's use of fingerprints for time tracking failed to allege a concrete injury); McGinnis v. United States Cold Storage, Inc., 382 F. Supp. 3d 813, 815-16 (N.D. Ill. 2019) (BIPA suit brought by employee against employer alleging noncompliant use of fingerprints for time tracking dismissed for failing to allege a concrete injury); Rivera v. Google, 366 F. Supp. 3d 998, 1001, 1014 (N.D. Ill. 2018) (BIPA suit brought by consumers against technology company for noncompliant use of face scans in social media product dismissed because plaintiffs had not suffered concrete injuries); McCullough v. Smarte Carte, Inc., 2016 WL 4077108 at *1, *4 (N.D. Ill. Aug. 1, 2016) (consumer who brought suit against locker rental company for BIPA violations in use of fingerprints had no concrete injury sufficient to satisfy Article III standing); *but see* Figueroa v. Kronos Inc., 2020 WL 1848206 (N.D. Ill. Apr. 13, 2020) (plaintiffs sufficiently alleged a concrete informational injury to confer Article III standing).

138. 958 F.3d 617, 619 (7th Cir. 2020).

139. 740 ILL. COMP. STAT. 14/15(b) (2018).

140. *Bryant*, 958 F.3d at 626.

141. 740 ILL. COMP. STAT. 14/15(a) (2018).

142. *Bryant*, 958 F.3d at 626.

the court found standing for allegations of failure to develop, adhere to, or disclose a deletion policy and retention schedule,[143] and *Thornley v. Clearview AI*, where it found insufficient standing for federal jurisdiction in alleged violations of BIPA's ban on profit from or sale of biometrics.[144]

D. Cases Involving Standing

1. *Santana v. Take-Two Software*

S*antana vs. Take-Two Software, Inc.* is one of the earlier BIPA cases, having been heard by the Second Circuit in 2017.[145] The case was an appeal by the plaintiffs of the district court's decision to grant the defendant's motion to dismiss.[146] The plaintiffs alleged that the defendant, a video game publisher, failed to gather consent to collect and disseminate their biometric information, to provide the proper notice required by BIPA as to the purpose of the collection and the duration of retention of the biometric data, and to protect their biometric data using a reasonable standard of care in storage and transmission.[147] The case centered around the "MyPlayer" feature found in two of Take-Two's "NBA 2K15" and "NBA 2K16" video games.[148] The feature allowed players to create an avatar in the game whose face was a realistic version of their own.[149] To utilize this feature, players first were required to agree to Take-Two's terms and conditions,[150] then placed their faces approximately one foot away from a camera while slowly turning their heads to the left and right for about fifteen minutes, allowing the game to scan the facial geometry necessary to create their personalized avatar.[151]

The plaintiffs, players of NBA 2K15 who used the MyPlayer feature, brought five claims under BIPA that can be grouped into three distinct violations: consent, notice, and security. The consent claims alleged that the defendant both collected the plaintiffs' biometric data and disseminated it to others without consent.[152] The notice claims alleged violations of BIPA's requirements to inform (in writing) the purpose of biometric collection, length the data will be stored, and to maintain a publicly-available schedule detailing

143. 980 F.3d 1146, 1148–49 (7th Cir. 2020).

144. 984 F.3d 1241, 1242 (7th Cir. 2021).

145. 717 F. App'x. 12, 12 (2d Cir. 2017).

146. *Id.* at 14–15.

147. *Id.* at 14.

148. *Id.* at 13.

149. *Id.*

150. The terms and conditions stated: "Your face scan will be visible to you and others you play with and may be recorded or screen captured during gameplay. By proceeding you agree and consent to such uses and other uses pursuant to the End User License Agreement. www.take2 games.com/eula." *Santana*, 717 F. App'x. at 13–14.

151. *Id.* at 14.

152. *Id.* at 13.

the retention and permanent destruction of the data.[153] Finally, the security claim alleged Take-Two's failure to protect the plaintiffs' biometric data with a reasonable standard of care as stringently as it protects other confidential or sensitive information, as required under BIPA.[154]

To determine whether there was Article III standing for a procedural violation of a statute, the court first reviewed the scope and purpose of the procedural right provided by the statute. The court assumed (without deciding) that "BIPA's purpose is to prevent the unauthorized use, collection, or disclosure of an individual's biometric data," identifying this purpose—the prevention of the unauthorized use, collection, or disclosure of biometric data—as the concrete interest protected by the statute.[155] This is similar to the court below, which found that "[t]he only concrete interest protected by the BIPA is biometric data protection."[156] Therefore, to find Article III standing, the court stated that the plaintiffs must prove that either "their biometric data [was] collected or disseminated without their authorization or . . . a procedural violation creates a material risk of such an outcome."[157]

Next, the court examined whether any of the alleged procedural BIPA violations raised a material risk of harm to the plaintiffs' interests (i.e., if the plaintiffs' "biometric data [was] collected or disseminated without their authorization or if a procedural violation creates a material risk of such an outcome").[158] The court quickly dismissed the allegations that BIPA's consent provisions were violated and held that the Take-Two's terms and conditions were sufficient under the circumstances to meet BIPA's requirement that individuals be informed in writing that their biometric information was being collected or stored.[159] The plaintiffs were required to agree to these terms to move forward and their participation in the relatively laborious, fifteen-minute-long face scan following that agreement further demonstrated their consent.[160] Because they were unable to demonstrate that the allegedly flawed terms and conditions caused them to consent to biometric collection where they otherwise would not have, the court found they had failed to allege a material risk of harm to their concrete interests here.

153. *Id.* at 13.

154. *Id.* at 13.

155. *Santana*, 717 F. App'x. at 15.

156. Virgil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 514 (S.D.N.Y. 2017).

157. *Santana*, 717 F. App'x. at 15.

158. *Id.*

159. *Id.* at 15–16. The terms and conditions for the MyPlayer feature referred to a "face scan" while BIPA defined a biometric identifier as a "scan of . . . face geometry" in § 14/10. Presumably, the court reasoned that including the word "geometry" so that the terms and conditions referred to a "face geometry scan" would have made the written consent more clearly compliant with the Act. *See id.* at 15.

160. *Id.* at 15–16.

Examining the notice claims, which alleged that Take-Two did not inform the plaintiffs of the duration for which it would store their biometric data or maintain a schedule for the data's retention and destruction, the court again found no risk of material harm to the plaintiffs' interests. While Take-Two may not have stated how long the biometric information would be stored, the court held that there was no allegation that they would not destroy the data as required.[161] The court further found that despite Take-Two's failure to post a schedule of biometric data retention and destruction, the plaintiffs "do not allege that Take-Two lacks such protocols, that its policies are inadequate, or that Take-Two is unlikely to abide by its internal procedures."[162] The court essentially concurred with the district court, which succinctly summarized its finding that procedural violations are not sufficient to constitute an injury-in-fact, stating that "a private entity may destroy biometrics pursuant to the requirements set forth in section 15(a), and thus effectively comply with the core data protection goal of the BIPA while also technically violating the BIPA by failing to publish a retention schedule."[163]

Finally, the court was left with the security claim, the allegations that Take-Two violated BIPA's data security provisions, which it stated "raise a somewhat thornier issue."[164] The plaintiffs alleged that their face scans were sent unencrypted via the open Internet—i.e., not via a secure, private network—in violation of BIPA's requirement to use a reasonable standard of care to protect biometric data in an entity's possession.[165] The court below rejected this argument, stating that while Take-Two may not have taken the steps to meet the requirements of BIPA in its storage and transmission of the biometrics, the allegations "[did] not establish an imminent risk that [the plaintiffs'] biometrics could actually be misused, and there has been no event, such as [a] data theft . . . that could make any such risk rise above the abstract level."[166] The trial court found this to be too abstract and speculative to confer standing.[167] The district court further rejected the argument that the harms involved with face scans are greater because they are unchangeable, unlike other information such as passwords, stating that the "hypothetical magnitude" of an injury that is still "highly speculative and abstract" and "not certainly impending" does not change

161. *Santana*, 717 F. App'x. at 16. BIPA calls for destruction of an individual's biometric data when the initial purpose for collecting the data has been satisfied or 3 years after the individual's last interaction with the entity collecting the biometric data, whichever occurs first. 740 ILL COMP. STAT. § 14/15(a) (2018).

162. *Santana*, 717 F. App'x. at 16.

163. Virgil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 514 (S.D.N.Y. 2017).

164. *Santana*, 717 F. App'x. at 16.

165. *Id.* at 17.

166. *Virgil*, 235 F. Supp. 3d at 511.

167. *Id.* at 512.

the analysis.[168] On appeal, the Second Circuit declined to engage in a similarly deep analysis on the security claim. It did, however, disagree with the defense's assertion that there is only standing when there has been an actual data breach.[169] It again found that the plaintiffs failed to show a real risk of harm sufficient to constitute an injury-in-fact, and affirmed the district court's dismissal for lack of Article III standing.[170]

2. *Patel v. Facebook*

In *Patel v. Facebook, Inc.*, the Ninth Circuit heard an appeal of a district court decision granting class certification against the plaintiffs, Illinois Facebook users, who brought a putative class action suit against the social networking giant Facebook alleging BIPA violations.[171] The Ninth Circuit, like the Second Circuit in *Santana*, applied the *Spokeo* guidance using a two-step approach to determine whether the violation of a statute causes a concrete injury.[172] The court asked (1) whether the statutory provisions at issue were established to protect the plaintiff's concrete interests (as opposed to purely procedural rights) and, if so, (2) whether the specific procedural violations alleged in the case constituted actual harm, or presented a material risk of harm to such interests.[173] Unlike the Second Circuit, the Ninth Circuit found that the *Patel* plaintiffs had alleged a concrete and particularized harm sufficient to confer Article III standing.[174]

In *Patel*, the defendant's alleged BIPA violations involved the "tag suggestions" feature on Facebook, which was launched in 2010.[175] If tag suggestions are enabled, when a user uploads a photo, facial recognition technology is employed to analyze the faces in that photo to determine whether they match any of the user's friends' faces.[176] This is accomplished by detecting images of faces in the photo, extracting the facial geometry of those faces, and comparing each face to Facebook's database of user face templates.[177] If there is a match, Facebook suggests the user tag that person in the photo.[178] While

168. *Id.*

169. *Santana*, 717 F. App'x. at 16.

170. *Id.* at 16–17.

171. 932 F.3d 1264, 1268–70 (9th Cir. 2019).

172. *Id.* at 1270–71.

173. *Id.* at 1270–71.

174. *Id.* at 1275.

175. *Id.* at 1268.

176. Sriivas Narayanan, *An Update About Face Recognition on Facebook*, FACEBOOK NEWSROOM (Sept. 3, 2019), https://about.fb.com/news/2019/09/update-face-recognition/ [https://perma.cc/EQ4A-TW5S].

177. Patel v. Facebook, Inc., 932 F.3d 1264, 1268 (9th Cir. 2019).

178. Blake Montgomery, *Facebook Makes Facial Recognition Opt-In Instead of Automatically Scanning Users' Faces*, THE DAILY BEAST (Sept. 03, 2019), https://www.thedailybeast.com/facebook-makes-facial-recognition-opt-in-gets-rid-of-tag-suggestions-system?ref=scroll

users could disable the "tag suggestions" feature, there was no information on the Facebook website that indicated that this could or would stop Facebook from collecting and using facial recognition data.[179] The "tag suggestions" feature has since been eliminated from Facebook, having been replaced in 2019 by a feature termed "face recognition" by Facebook that utilizes facial recognition to alert users if their profile photo is used by someone else or if they appear in photos in which they are not tagged.[180] "Face recognition" also continues to suggest users tag friends when they upload a photo, just as "tag suggestions" did, but the new feature allows users to opt-out, in which case Facebook will not store their face template nor use facial recognition to identify them in photos.[181] Illinois Facebook users brought suit, alleging Facebook collected, used, and stored their biometric identifiers—scans of their face geometry—without securing a written release or posting a compliant retention schedule for the biometric identifiers, in violation of BIPA.[182]

To begin its analysis, the court—similarly to the *Santana* court—considered whether the BIPA provisions at issue protect a concrete interest or mere procedural rights.[183] To do so, the court first embarked on a brief history of the protection of privacy by the law in both American and English courts, noting that "common law privacy rights are intertwined with constitutionally protected zones of privacy."[184] The court then detailed the Supreme Court's recent jurisprudence on the potential of new technologies to violate privacy rights and discussed the Illinois General Assembly's intent when BIPA was introduced.[185] Ultimately, the court concluded that BIPA protects individuals' concrete interest in privacy.[186] This is notably broader than the *Santana* court's determination that the concrete interest protected by BIPA is an individual's interest in preventing

[https://perma.cc/4EN3-Q5QF]. A tag identifies the friend in the photo by name and includes a link to that friend's Facebook profile. *What is Tagging and How Does it Work?*, FACEBOOK HELP CENTER, https://www.facebook.com/help/124970597582337?helpref=uf_permalink [https://perma.cc/C8B3-VSJ4].

179. Thomas Germain, *Facebook Updates Facial Recognition Settings After CR Investigation*, CONSUMER REPORTS (Sept. 03, 2019), https://www.consumerreports.org/privacy/facebook-updates-facial-recognition-setting/ [https://perma.cc/ALL4-MJDH].

180. Jon Swartz, *Facebook Makes Face Recognition Available to All Users, Spikes Tag Suggestions*, MARKETWATCH (Sept. 3, 2019), https://www.marketwatch.com/story/facebook-makes-face-recognition-available-to-all-users-spikes-tag-suggestions-2019-09-03 [https://perma.cc/ZB6Y-N3FZ].

181. *What is the Face Recognition Setting on Facebook and How Does it Work?*, FACEBOOK HELP CENTER, https://www.facebook.com/help/122175507864081?helpref=faq_content [https://perma.cc/95FM-47YL].

182. Patel v. Facebook, Inc., 932 F.3d 1264, 1268 (9th Cir. 2019).

183. *Id.* at 1271.

184. *Id.* at 1272.

185. *Id.* at 1272–74.

186. *Id.* at 1274.

the unauthorized collection, use, or dissemination of their biometric data, because the Ninth Circuit frames the interest as *maintaining* privacy, versus merely *preventing* violations of privacy.

In the second part of the analysis, determining whether the procedural violations actually harmed or presented a material risk of harm to the concrete interest at play, the *Patel* court again differed from the *Santana* court. The court characterized the privacy right that BIPA protects as "the right not to be subject to the collection and use of . . . biometric data."[187] Therefore, the court reasoned, because the allegations were that Facebook collected, used, and stored such biometric data without following the procedures required by the statute, a failure to follow these procedures must violate the substantive privacy interests of the plaintiffs, representing sufficient concreteness to confer Article III standing.[188]

This appears directly in conflict with the *Santana* court's decision that standing requires some other non-abstract harm or material risk of harm to a concrete interest beyond the statutory violation itself. This conflict stems from the differing conclusions each court reaches in identifying the concrete interest protected by BIPA. The concrete interest found by the Second Circuit, the interest in preventing the unauthorized collection, use, or disclosure of biometric data, is more difficult to allege as a violation because a plaintiff must allege not merely a procedural or technical violation of the statute but an actual, or material risk of, unauthorized collection, use, or disclosure of his biometric data in order to have standing. On the other hand, the broader concrete interest found by the Ninth Circuit to be protected by BIPA—the interest in one's privacy—is easier to allege as a procedural violation because any failure to adhere to a statutory provision must then harm the concrete interest in privacy protected by the provision.

Facebook appealed the Ninth Circuit's decision to the Supreme Court, arguing that review was warranted due to the deepened circuit split on standing.[189] The Supreme Court, however, denied certiorari in January 2020.[190] Out of options, Facebook settled the suit for $550 million,[191] an amount which ultimately grew to $650 million by the time the settlement received court

187. *Patel*, 932 F.3d at 1274.

188. *Id.*

189. *See* Petition for a Writ of Certiorari at 6, Facebook, Inc. v. Patel, No. 19-706, 2019 WL 6640455 (U.S. Dec. 2, 2019).

190. *See* Facebook, Inc. v. Patel, No. 19-706, 2020 WL 283288 (Mem) (U.S. Jan. 21, 2020).

191. Natasha Singer & Mike Isaac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020), https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html [https://perma.cc/8ATZ-5KPC].

approval.[192] This settlement led commentators to note the effectiveness of BIPA in protecting consumer privacy rights.[193]

3. *Miller v. Southwest Airlines*

At the time of the *Patel* decision, the Seventh Circuit had only ruled on standing in BIPA litigation in an employment case, *Miller v. Southwest Airlines*, where it affirmed the district court's finding that the plaintiffs had Article III standing but primarily focused its analysis on jurisdictional concerns.[194] In *Miller*, a consolidated appeal of two cases, one brought against United Airlines by its employees and another against Southwest Airlines by its employees, the plaintiff-employees alleged violations of BIPA in the airlines' use of timekeeping systems that required employees to scan their fingerprints in order to clock in and out of work.[195] The plaintiffs alleged that the employers did not receive employees' consent to use their biometric information, as required by section 15(b)(3) of the Act, nor did they publish a publicly-available policy regarding the retention and destruction of biometric identifiers and information, as required by section 15(a).[196] Further, the airlines allegedly used third-party vendors to manage their timekeeping systems, which was an alleged disclosure prohibited by section 15(e)(1),[197] which requires entities in possession of biometric identifiers or biometric information to "protect [the biometric identifier or biometric information] from disclosure."[198] At the district court level, the two suits were assigned to different judges, one of whom found the plaintiffs to have standing under Article III, while the other remanded the case to state court, noting that the "complaint did not present a case or controversy, because the class asserted only a bare procedural right."[199]

Though the reasoning is only applicable in employment cases involving specific federally-regulated industries, the Seventh Circuit held that plaintiffs had standing to sue and that the use of fingerprint identification for timekeeping amounted to a material change in the unionized workers' terms and conditions

192. Jake Holland, *Facebook's $650 Million Privacy Settlement Approved by Judge*, BLOOMBERG LAW (Feb. 26, 2021, 3:23 PM), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X40VSPS8000000 [https://perma.cc/N3RT-B4JA].

193. *See* Allison Grande, *Record Facebook Deal May Boost US Privacy Law Push*, LAW360 (Jan. 31, 2020, 9:35 PM), https://www.law360.com/articles/1239728/ [https://perma.cc/SUN3-BJZF]. This includes the federal judge overseeing the settlement, who noted that Facebook's "settlement is a major win for consumers in the hotly contested area of digital privacy." In re Facebook Biometric Information Privacy Litigation, No. 15-cv-03747-JD, 2021 WL 757025, at *1 (N.D. Cal. Feb. 26, 2021).

194. 926 F.3d 898, 905 (7th Cir. 2019).

195. *Id.* at 900–01.

196. *Id.* at 901.

197. *Id.*

198. 740 ILL. COMP. STAT. 14/15(e)(1) (2018).

199. *Miller*, 926 F.3d at 902.

of employment that satisfied the concreteness requirement of Article III, allowing a court or adjustment board to order changes in clocking in and out if they were to find that the unions had not consented.[200] The court proceeded to analyze the plaintiffs' allegations that the carriers were not following the Act's data-retention and destruction procedures and were using third-party vendors.[201] Noting that "the longer data are retained, and the more people have access, the greater the risk of disclosure," the court emphasized that there was no indication that the data had, in fact, reached any malevolent third party, and declined to reach a conclusion on whether "risk of disclosure itself suffices for standing," leaving the question unresolved.[202]

4. *Bryant v. Compass Group USA*

In *Bryant v. Compass Group USA*, the Seventh Circuit joined the Ninth and Second Circuits in ruling on a BIPA claim in a consumer context: this case involved the defendant vending machine operator's alleged use of the plaintiff's fingerprints in violation of BIPA.[203] The vending machine, available at plaintiff's workplace, did not accept cash and instead required users to establish an account using a fingerprint to authenticate their identity.[204] Using their fingerprints, employees could purchase items and add money to their accounts.[205]

The plaintiff alleged several violations: 1) the defendant failed to inform users that their biometric identifiers (fingerprints) were being collected or stored; 2) the defendant failed to inform users of the purpose and length of the term of the collection; and 3) the defendant failed to obtain a written release to collect, store, and use the fingerprints.[206] Interestingly, the plaintiff made clear that this was a suit alleging a bare procedural violation: the court noted that "Bryant [did] not assert that she did not know that her fingerprint was being collected and stored, nor why this was happening," merely that the defendant failed to comply with the provisions of the Act which resulted in "the loss of [her] right to control [her] biometric identifiers and information."[207]

The plaintiff brought a putative class action in Illinois state court, at which point the defendant removed the action to federal court under CAFA, on the basis of diversity of citizenship (the defendant being a Delaware corporation with its principal place of business in North Carolina, and the plaintiff being a citizen of Illinois) and an amount in controversy of over five million dollars (the

200. *Id.*
201. *Id.*
202. *Id.* at 902–03.
203. 958 F. 3d 617, 620 (7th Cir. 2020).
204. *Id.* at 619.
205. *Id.*
206. *Id.*
207. *Id.* at 620.

defendant asserted that the class had at least 1,000 members, each of whom would be authorized under BIPA for statutory damages of $5,000 per intentional or reckless violation).[208]

The court first applied *Spokeo* and concluded that "[a] direct application of *Spokeo* . . . leads to the result that [the plaintiff] satisfied the injury-in-fact requirement of Article III."[209] Because the case asserted a violation of the plaintiff's rights in "her fingerprints, her private information,"[210] the defendant's failure to adhere to BIPA's requirements constituted an invasion of the plaintiff's private domain similar to an act of trespass, satisfying *Spokeo*'s requirement that a plaintiff allege a concrete and particularized harm to possess Article III standing.[211]

The court also analyzed the case "as a type of informational injury," where it also found standing.[212] It first examined its recent decision in *Groshek v. Time Warner Cable*, where the prospective employee sued because the employer failed to give applicants a stand-alone written disclosure that a consumer report may be obtained, in violation of the FCRA.[213] The disclosure was instead contained on a document alongside other information.[214] Because the *Groshek* plaintiff did not allege he was not able to give knowing and informed consent due to the disclosure not being a stand-alone document, the Seventh Circuit held he did not allege a concrete injury.[215]

The court then contrasted *Groshek* with its decision in *Robertson v. Allied Solutions*, *LLC*, where a company failed to provide a prospective employee with a copy of her consumer report before it rescinded her employment offer because of information contained in the report.[216] This was sufficient to constitute an injury-in-fact to sue under the FCRA because the plaintiff "was wholly deprived of the information necessary to respond in the way FCRA contemplated."[217]

The injury alleged in the *Bryant* case, the court reasoned, was quite similar to that alleged in *Robertson*.[218] The defendant's failure to adhere to BIPA's requirements "denied [the plaintiff] and others like her the opportunity to consider whether the terms of [the] collection and usage [of fingerprints] were

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

209. *Id.* at 624.

210. *Id.*

211. *See id.*

212. *Id.*

213. *Bryant*, 958 F. 3d at 625 (citing Groshek v. Time Warner Cable, 865 F.3d 884, 886 (7th Cir. 2017)).

214. *Id.* (citing *Groshek*, 865 F.3d at 886).

215. *Groshek*, 865 F.3d at 889.

216. *Bryant*, 958 F.3d at 625 (citing Robertson v. Allied Solutions, LLC, 902 F.3d 690, 696 (7th Cir. 2018)).

217. *Id.*

218. *Id.* at 626.

acceptable given the attendant risks."[219] Thus, the defendant's violation of BIPA section 15(b) went beyond a purely procedural requirement in that it withheld substantive information from the plaintiff, depriving her of the ability to make informed consent.[220]

The Seventh Circuit, however, did not join the Ninth Circuit in finding standing for a violation of BIPA section 15(a), the provision of BIPA that requires companies to have a publicly available policy concerning their retention of biometric information as well as a deletion schedule.[221] It held that this is a duty "owed to the public generally, not to particular persons whose biometric information the entity collects."[222] Thus, it did not form part of BIPA's "informed-consent regime" and the plaintiff did not allege any particularized harm from this violation, meaning she lacked standing under Article III to bring suit in federal court for that claim.[223]

While the *Bryant* decision may have given weight (in light of the Ninth Circuit's *Patel* ruling) to the theory that procedural violations of BIPA section 15(b) concerning notification and consent are sufficient to confer federal standing, *Bryant* differed from *Patel* in that it distinguished BIPA section 15(a) (concerning destruction and retention schedules) where it did not find standing for mere procedural violations. The *Patel* decision only held that alleged violations of section 15 more broadly, without differentiating between the different subsections, were sufficient to confer standing.[224] However, it is important to note that the *Bryant* plaintiff's allegation of a BIPA section 15(a) violation was limited to the defendant's failure to *develop* a written schedule of retention and deletion available to the public.[225] The Seventh Circuit, stating its "analysis [was] limited to the theory [the plaintiff] invoked," explicitly did not rule on standing based on a defendant's alleged violation of section 15(a)'s requirement for *compliance* with its *already-established* retention and deletion schedules, thus leaving the door open for potential additional routes to standing in future cases.[226]

5. *Fox v. Dakkota Integrated Systems*

The continuing surge in BIPA class action claims[227] quickly provided the Seventh Circuit with several cases following *Bryant* that allowed the court to

219. *Id.*
220. *Id.*
221. *Bryant*, 958 F.3d at 626.
222. *Id.*
223. *Id.*
224. *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1274–75 (9th Cir. 2019).
225. *Bryant*, 958 F.3d at 626.
226. *Id.*
227. *See* Maatman, Jr. et al., *supra* note 69; *see also* Tiffany Cheung, Michael Burshteyn, & Camille Framroze, *Privacy Litigation 2020 Year in Review: BIPA Litigation*, MORRISON

expand its BIPA jurisprudence. The first came in *Fox v. Dakkota Integrated Systems*.[228] The *Fox* plaintiff alleged that her employer violated BIPA by requiring employees to use biometric information (fingerprints) to clock in and out of work.[229] The plaintiff alleged her employer did not receive her written consent to collect the biometric information, in violation of BIPA section 15(b), and that it did not receive her written consent when it disseminated her biometric information to the third-party company that managed the time-keeping software and the storage of the time records in a database, in violation of section 15(d).[230] Additionally, the *Fox* plaintiff alleged violations of section 15(a) that were broader than those alleged in *Bryant*: here, the plaintiff did not just allege a failure to disclose a data-retention policy, but also alleged the defendant failed to even develop a data-retention policy and that it failed to comply with a data-retention policy and guidelines to permanently destroy the biometric information once it was no longer needed.[231]

These allegations allowed the court to continue its Article III standing discussion regarding BIPA's requirements to develop, comply with, and make publicly available a data-retention schedule right where *Bryant* left off: while the *Bryant* court held that the bare allegation of failing to publicly disclose a data-retention schedule publicly was insufficient to confer Article III standing to sue for BIPA section 15(a) violations,[232] what about allegations of failure to develop and comply with a data-retention policy? That is what was alleged in *Fox*.[233]

In *Fox*, the court ruled that the 15(a) allegations were sufficient to confer Article III standing,[234] stating that "[t]he BIPA requirement to implement data retention and destruction protocols protects a person's biometric privacy just as

FOERSTER (Jan. 12, 2021), https://www.mofo.com/resources/insights/210111-bipa-litigation.html [https://perma.cc/YG72-KWGD] ("In 2020, at least 54 court rulings referenced BIPA. This is more than double 2019's count."); Marsh, *supra* note 97 (noting that, as of November 2020, there have already been 58 federal complaints alleging BIPA claims in 2020, more than 2018 and 2019 combined).

228. 980 F.3d 1146, 1146 (7th Cir. 2020).

229. *Id.* at 1149–50.

230. *Id.* at 1150. Because the *Fox* plaintiff was represented by a union, her claims alleging violations of BIPA sections 15(b) and 15(d) were preempted by the Labor Management Relations Act and dismissed by the district court; the appellate court's decision focused on the Article III standing of the plaintiff's 15(a) claim. *Id.* at 1150–51.

231. *Id.* at 1150.

232. Bryant v. Compass Group USA, Inc., 958 F.3d 617, 626 (7th Cir. 2020).

233. *See* Class Action Complaint at 16-17, Fox v. Dakkota Integrated Systems, LLC, No. 1:19-cv-02872 (N.D. Ill. Apr. 29, 2019), ECF No. 1-1, 2020 WL 8409682 (alleging that the defendant failed to comply with BIPA's mandate to establish, comply with, and make publicly available a schedule for retention and deletion of biometric data, that it does not have any retention schedule or deletion guideline for biometric data, and that it had not and would never destroy the plaintiff's biometric data in its possession).

234. *Fox*, 980 F.3d at 1156.

concretely as the statute's informed consent regime."[235] Given that it had held in *Bryant* that violations of this informed-consent regime, found in BIPA section 15(b), represented a concrete and particularized injury sufficient to confer standing,[236] it reasoned that the *Fox* plaintiff's allegations of unlawful retention of biometric data was an injury equally concrete and particularized as the unlawful collection of biometrics.[237] The court noted that the 15(a) violations alleged in *Bryant* were "extremely narrow" while the *Fox* plaintiff's 15(a) claim was "much broader."[238] This distinction will likely be important for BIPA suits going forward—alleging that a defendant failed to publicly disclose a data-retention policy and destruction schedule for biometric data is not enough; under the Seventh Circuit's *Fox* reasoning, plaintiffs must also allege the defendant failed to develop such a policy and failed to adhere to it.

The court also differentiated between biometric identifiers and other consumer data (such as telephone, credit card, and social security numbers) at issue in past cases involving procedural violations of statutes, noting that biometrics are immutable and thus inherently sensitive.[239] Thus, a violation of BIPA section 15(a) by failing to delete biometrics as required by the law is "closely analogous to historical claims for privacy."[240] The court reversed the district court's remand order, allowing the 15(a) claims to be litigated in federal court.[241]

6. *Thornley v. Clearview AI*

The next BIPA case considered by the Seventh Circuit, *Thornley v. Clearview AI, Inc.*,[242] arrived before the court with the plaintiff arguing *against* her own federal standing and the defendant advocating *for* the plaintiff's standing to sue, "for reasons that only a civil procedure buff could love."[243] The facts of the case concern Clearview AI's facial recognition tool that harvests publicly-available pictures from social media sites in order to develop biometric facial scans of individuals that it then stores on a database.[244] Clearview AI's business is centered around selling access to its facial-recognition technology, which allows its customers (mostly law enforcement agencies) to identify unknown persons in photographs by uploading photographs to a Clearview website, where Clearview's facial-recognition technology creates a facial scan

235. *Id.* at 1155.
236. *Bryant*, 958 F.3d at 626–27.
237. *Fox*, 980 F.3d at 1154–55.
238. *Id.* at 1154.
239. *Id.* at 1155.
240. *Id.* (quoting *Bryant*, 958 F.3d at 623).
241. *Id.* at 1156.
242. 984 F.3d 1241, 1241 (7th Cir. 2021).
243. *Id.* at 1242.
244. *Id.* at 1242–43.

for the person in the photograph, compares this scan to the facial scans stored in its database, and, if there is a match, directs the user to the social media profile of the individual identified.[245]

The procedural history of the case is quite interesting. The plaintiff filed the class-action suit in Illinois state court, alleging violations of three BIPA provisions.[246] Clearview removed the case to federal court, and shortly thereafter the plaintiff voluntarily dismissed the suit.[247] The suit was then refiled in Illinois state court, this time "significantly narrowed" in its claims: the plaintiff now alleged only that Clearview violated BIPA's section 15(c), banning private entities from selling, leasing, trading, or profiting from biometric data, and included a "much more modest" class definition.[248] In this new suit, the plaintiff's proposed class specified that it included only those "who suffered no injury from Defendant's violation of [s]ection 15(c) of BIPA other than statutory aggrievement."[249] Clearview again removed the case to federal court, where the district court held there was no Article III standing and remanded the case to state court.[250] Clearview appealed, resulting in the case before the Seventh Circuit.[251]

In its analysis of section 15(c), the court noted that the bare allegations of the plaintiff "raised questions only about a general regulatory rule found in BIPA."[252] While Clearview urged the court to focus on the potential injury of selling, leasing, profiting from a person's biometric data, the court noted that this was not the allegation in the actual complaint.[253] It noted that federal standing could perhaps be found where a hypothetical plaintiff alleged 15(c) violations and argued that a defendant "has deprived her of the opportunity to profit from her biometric information."[254] However, the court noted, in the actual case at bar, the plaintiff alleged only a violation of a "general regulation"

245. *Id.* at 1243. For more information about Clearview's business model and technology and discussion of the company's ramifications on society, see Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/NFT3-G6FJ].

246. *Thornley*, 984 F.3d at 1243. The plaintiff alleged violations of sections 15(a), 15(b), and 15(c) of BIPA. *Id.* These provisions include the requirement to develop and make publicly available retention schedules and destruction guidelines for biometric data (15(a)), the requirement to receive a written release prior to the collection of biometric information (15(b)), and the ban on selling, leasing, trading, or otherwise profiting from biometric data (15(c)). *See* 740 ILL. COMP. STAT. 14/15 (2020).

247. *Thornley*, 984 F.3d at 1243.

248. *Id.*

249. *Id.* at 1246.

250. *Id.* at 1243.

251. *Id.* at 1242.

252. *Thornley*, 984 F.3d at 1246.

253. *See id.* at 1246–47.

254. *Id.* at 1247.

found in BIPA, and, similar to the 15(a) claim made by the plaintiff in *Bryant*, asserted no particularized injury.[255] Ultimately, the court concluded that while the plaintiff clearly crafted the complaint to avoid federal court, plaintiffs are allowed to do so, and because the complaint's allegations described no particularized or concrete injury, the case lacked the Article III standing required to be pursued in federal court and the district court's remand was proper.[256]

The implications of this decision on BIPA litigation moving forward are likely to be significant, as the court gave its stamp of approval to claims deliberately crafted to avoid federal courts if the plaintiff so wishes. Commentators have noted that the court has, essentially, provided plaintiffs with a "road map" for avoiding federal courts: by "restricting [complaints] to bare statutory violations," plaintiffs can ensure their BIPA suits are litigated in Illinois state courts.[257]

III. POTENTIAL SUPREME COURT INTERPRETATION & ANALYSIS OF IMPACT

A. Why the Court Should Find Standing for Procedural Violations

As of this writing, there is no BIPA litigation pending appeal to the Supreme Court, as Facebook's petition for writ of certiorari from the Ninth Circuit's *Patel* decision was denied by the Court,[258] though it appears likely that Clearview AI will be appealing the Seventh Circuit's *Fox* decision.[259] With the Seventh Circuit's ruling in *Bryant*, the pendulum seems to be swinging towards a more permissive regime for finding Article III standing for statutory data-privacy violations alone—at least in BIPA cases. Given the Court's jurisprudence in *Spokeo*, it seems that were it to resolve the circuit split on BIPA standing, it would be appropriate for the Court to find Article III standing in situations involving procedural violations of BIPA's notification, consent, and disclosure provisions.

There are two pertinent inquiries to make here. The first inquiry regards the legislative intent behind the procedural rights BIPA established. In *Spokeo*, the Court noted that when determining whether an intangible harm, such as a procedural violation of BIPA, constitutes injury in fact, "both history and judgment of Congress play important roles."[260] Here, where a state law is at issue, the judgment of the promulgating legislature should be examined. The Second Circuit assumed "that BIPA's purpose is to prevent the unauthorized

255. *Id.*

256. *Id.* at 1248–49.

257. *See* Marsh, *supra* note 97.

258. *See* Facebook, Inc. v. Patel, No. 19-706, 2020 WL 283288 (Mem) (U.S. Jan. 21, 2020).

259. *See* Clearview AI, Inc.'s Motion to Stay the Mandate Pending the Filing and Resolution of a Petition for a Writ of Certiorari, Thornley v. Clearview AI, Inc., No 20-3249 (7th Cir. Feb. 22, 2021), ECF No. 47.

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

use, collection, or disclosure of an individual's biometric data."[261] The Ninth Circuit, on the other hand, determined that "the statutory provisions at issue in BIPA were established to protect an individual's 'concrete interests' in privacy, not merely procedural rights."[262] Similarly, the Seventh Circuit held that the plaintiff "was asserting a violation of her own rights—her fingerprints, her private information—and [] this is enough to show injury-in-fact without further tangible consequences."[263] Reading the plain text of the legislative intent of the Act, which states that "[t]he public welfare, security, and safety will be served by regulating . . . biometric identifiers and information" and that "[b]iometrics are unlike other unique identifiers . . . [because] once compromised, the individual has no recourse." [264] Both the Ninth and Seventh Circuits read this to determine that the Illinois legislature intended to establish privacy rights in individuals' biometric information. The Illinois Supreme Court stated in *Rosenbach* that "our General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information."[265] The Supreme Court should affirm this interpretation and find that BIPA created a statutory right in biometric privacy.

This brings us to our second inquiry—whether the risk of harm in situations such as these is sufficient in the Court's eyes to satisfy the requirement of concreteness, and thus to constitute standing. In *Spokeo*, the Court noted that it is possible for the "risk of real harm" to constitute a concrete injury.[266] In these types of cases, the Court noted, plaintiffs "need not allege any additional harm beyond the one Congress has identified."[267] Both the Ninth and Seventh Circuits looked to the *Rosenbach* decision for insight into the risk of real harm when procedural BIPA violations were at issue. The *Rosenbach* court stated that the procedural requirements of BIPA "are particularly crucial in our digital world" because when a private entity "fails to adhere to the statutory procedures . . . the right of the individual to maintain his or her biometric privacy vanishes into thin air."[268] This seems sufficient enough to constitute the "risk of real harm" the Court discussed in *Spokeo*, and thus the Court should hold there is sufficient risk of harm to satisfy the concreteness requirement when BIPA's provisions are violated—without showing any additional harm.

The Court may also evaluate BIPA standing from the perspective of its informational injury jurisprudence. In *Federal Election Commission v. Akins*, the Court held that a group of voters had standing to sue under the Federal

261. Santana v. Take-Two Interactive Software, Inc., 717 F. App'x. 12, 15 (2nd Cir. 2017).
262. *Patel*, 932 F.3d at 1274.
263. *Bryant*, 958 F.3d at 624.
264. 740 ILL. COMP. STAT. 14/5.
265. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1206 (Ill. 2019).
266. Spokeo, Inc. v. Robins, 136 S.Ct. 1540, 1549 (2016).
267. *Id.*
268. *Rosenbach*, 129 N.E.3d at 1206.

Election Campaign Act of 1971 ("FECA").[269] The plaintiffs sought to challenge the Federal Election Commission's determination that an organization was not a political committee under FECA, and thus not subject to FECA's requirements.[270] The Court held that the injuries suffered by plaintiffs—the "inability to obtain information" that they would be able to were the organization determined to be a political committee and thus subject to FECA's disclosure requirements—was sufficient to confer standing.[271] The Court noted that FECA was enacted with the intention to "protect voters such as respondents from suffering the kind of injury here at issue."[272] Similarly, in *Public Citizen vs. U.S. Dept. of Justice*, the plaintiffs sued under the Federal Advisory Committee Act ("FACA") after the American Bar Association ("ABA") refused requests for meeting minutes and committee reports related to its advisory role to the federal judiciary.[273] The plaintiffs argued that FACA should apply to the ABA, which would require it to make publicly available its documents such as the minutes and reports sought.[274] When the defendants sought to have the case dismissed for lack of standing, the Court declined to do so, stating that "the refusal to permit appellants to scrutinize the ABA Committee's activities to the extent FACA allows constitutes a sufficiently distinct injury to provide standing to sue."[275]

The common thread in these cases is that the statutory right afforded was a right to information that the plaintiffs were being denied. BIPA's disclosure requirement was characterized by the Seventh Circuit as a duty "owed to the public generally" when it held that the *Bryant* defendant's violation of that provision resulted in "no particularized harm" to the plaintiff.[276] This would seem to represent a possible conflict with *Public Citizen* and *Akins* and an opportunity for the Court to clarify that the BIPA disclosure provision creates a statutory right to information that, if denied, constitutes an informational injury sufficient to confer standing.

B. Potential Impact of a Supreme Court Decision on Standing for Procedural BIPA Violations

1. On BIPA Litigation in Federal Courts

If the Supreme Court instead resolved the standing split by finding no federal standing for procedural BIPA violations, the immediate impact would be

269. 524 U.S. 11, 14 (1998).
270. *Id.* at 13–14.
271. *Id.* at 21.
272. *Id.* at 20.
273. 491 U.S. 440, 447 (1989).
274. *Id.*
275. *Id.* at 449.
276. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 626 (7th Cir. 2020).

the inability of federal courts to hear these cases, outside of a data breach involving biometric information or other fact pattern where concrete harm may be more easily demonstrated. These types of claims would then be litigated exclusively in the Illinois state courts, where the *Rosenbach* decision ensures there is standing to sue for even bare procedural violations.[277] The Court could also find there is federal standing only for certain types of BIPA claims but not others. This would result in some BIPA claims moving forward in federal court while others (even those alleged in the same complaint) are remanded to Illinois state courts for resolution—as was the case in *Bryant*, where the Seventh Circuit found federal standing for the plaintiff's 15(b) claims, but not for her 15(a) claims.[278]

Given the absence of the standing issue in Illinois courts, potential plaintiffs seem to prefer to litigate BIPA claims there: it is the defendants who often remove these actions to the federal courts.[279] This could be because corporate defendants perceive federal courts to be more predictable, more transparent, and "less subject to local biases" than state courts,[280] which could lead to defendants removing more cases involving BIPA issues of first impression to federal, hoping for a decision that will benefit the defense bar.[281] It is more difficult to have a class certified in federal court than in state court,[282] and federal courts are more likely to grant motions to dismiss than state courts,[283] which could play

277. *See* discussion *infra* Section II.A.

278. *See* discussion *infra* Section II.D.4; *see also* Hazlitt v. Apple Inc., No. 3:20-CV0421-NJR, 2020 WL 6681374, at *4–7, *11 (S.D. Ill. Nov. 12, 2020) (remanding plaintiffs' claims under BIPA sections 15(a) and (c) to state court for lack of Article III standing, while finding Article III standing for and denying the defendant's motion to dismiss in regard to the claim under BIPA section 15(b)).

279. *See, e.g.*, Bryant v. Compass Grp. USA, Inc., 436 F. Supp. 3d 1087, 1088 (N.D. Ill. 2020) (stating that Plaintiff "filed this putative class action in the Chancery Division of Cook County Circuit Court" followed by, several months later, "Defendant [filing] a notice of removal in [federal district court] . . . "); Peatry v. Bimbo Bakeries USA, Inc., 393 F. Supp. 3d 766, 767 (N.D. Ill. 2019) (stating that Plaintiff "filed this putative class action lawsuit in state court" and the defendant subsequently "removed the case to federal court on the basis of diversity jurisdiction and the Class Action Fairness Act…" (citations omitted)); *see also* Marsh, *supra* note 97.

280. Colin E. Wrabley & Joshua T. Newborn, *Getting Your Company's Case Removed to Federal Court When Sued in Your 'Home' State*, LAW.COM (Dec. 19, 2017, 12:38 PM), https://www.law.com/thelegalintelligencer/sites/thelegalintelligencer/2017/12/19/getting-your-companys-case-removed-to-federal-court-when-sued-in-your-home-state/ [https://perma.cc/RH5L-ZMGY].

281. Rosa M. Tumialán, *A BIPA Defense Victory—If You Squint*, THE FIREWALL (Oct. 4, 2019), https://www.thefirewall-blog.com/2019/10/a-bipa-defense-victory-if-you-squint/ [https://perma.cc/Z6T5-ZGGG].

282. David Poell et al., *Beware BIPA Bifurcation: Plaintiffs' New Gambit to Split BIPA Claims Between State and Federal Court*, JDSUPRA (Mar. 17, 2021), https://www.jdsupra.com/legalnews/beware-bipa-bifurcation-plaintiffs-new-6284956/ [https://perma.cc/BKF4-G8A7].

283. *See* Max Kennerly, *Unanimous Supreme Court Resets "Principal Place of Business" For Diversity Jurisdiction*, LITIGATION & TRIAL (Feb. 24, 2010), https://www.litigationandtrial.com

into defendants' decisions as well. Whatever the reasons, a Supreme Court decision finding no standing for procedural BIPA violations would deprive corporate class-action defendants of a federal forum, seemingly counter to the purposes of CAFA, which was passed to *provide* a federal forum for such defendants.[284]

However, the current open question of federal standing for procedural violations ultimately allows both plaintiffs and defendants to delay the resolution of suits, and drive up litigation costs, and increase the burden on courts through strategic tactics deployed to obtain a party's desired forum.[285] Plaintiffs' attorneys may prefer the bifurcation of BIPA claims— where some are remanded to state court while others are litigated in federal court—because they can both obtain their preferred state court forum and simultaneously be litigating in two venues at once, which may be to their advantage.[286] It also increases defense costs and likely pressures defendants to settle. The current state of BIPA federal standing also encourages the type of strategy such as that found in *Thornley*, where the plaintiff's proposed class was limited to those suffering no injury "other than statutory aggrievement"[287] in order to avoid federal court, which may discourage defendants from remanding at all—or, it may encourage them to remand again, later, if the plaintiffs go on to "change their tune in state court," which the *Thornley* court hinted could allow defendants a chance at future removal back to a federal forum.[288] It may also discourage defendants from addressing standing as a threshold issue at all, instead saving it for class certification.[289]

On the other hand, clarifying that there *is* federal standing for procedural BIPA violations serves the interests of both plaintiffs and defendants: it would

/2010/02/articles/the-law/for-lawyers/unanimous-supreme-court-resets-principle-place-of-business-for-diversity-jurisdiction/ [https://perma.cc/9VPM-BHVF].

284. William Branigan, *Congress Changes Class Action Rules*, WASH. POST (Feb. 17, 2005, 3:55 PM), https://www.washingtonpost.com/wp-dyn/articles/A32674-2005Feb17.html [https://perma.cc/HN9U-LZ8J] ("[CAFA] had been strongly pushed by business groups, which argued that class-action lawsuits were enriching trial lawyers, who often filed them in certain jurisdictions known for sympathetic judges and juries.").

285. The plaintiffs in *In re Facebook Biometric Information Privacy Litigation* highlighted the bizarre position of the defendant, who was the party responsible for removing the case from state to federal court, stating that "[a]s the party asserting federal jurisdiction, Facebook maintains the burden to demonstrate that [the plaintiffs] have Article III standing, which it has now disavowed." Plaintiffs' Joint Response in Opposition to Facebook's Motion to Dismiss for Lack of Subject Matter Jurisdiction at 13, In re Facebook Biometric Privacy Litigation, No. 3:16-cv-00937-JD (N.D. Cal. Aug. 4, 2016), 2016 WL 4533593.

286. Poell et al., *supra* note 282.

287. Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1246 (7th Cir. 2021).

288. *Id.* at 1248.

289. Lincoln Wilson & Michael Fazio, *Defense Strategies When Plaintiffs Deny Their Own Standing*, LAW360 (Feb. 17, 2021, 5:05 PM), https://www.law360.com/articles/1354306/defense-strategies-when-plaintiffs-deny-their-own-standing [https://perma.cc/YTD2-JAYG].

allow both plaintiffs and defendants access to the federal court system, and allow federal courts to actually get to the merits of the suits. This could create benefits for both plaintiffs and defendants by litigating in a venue that may have more expertise and/or experience than state courts with cases involving data privacy, such as the Ninth Circuit, home to the headquarters of many technology corporations, while allowing defendants to access the federal courts and the benefits of diversity jurisdiction. It would encourage compliance with BIPA, providing entities using biometric data with "the strongest possible incentive to conform to the law and prevent problems before the occur and cannot be undone."[290] Most importantly, though, finding standing for procedural BIPA violations would affirm that violations of privacy rights granted by BIPA are, in fact, harms sufficiently injurious—concrete, particularized, and actual—to grant Article III standing. As the Illinois Supreme Court noted in *Rosenbach*, BIPA "vests in individuals and customers the right to control their biometric information" and a failure to adhere to the statute's provisions results in this right being taken from the individual—such a violation "is no mere 'technicality.'"[291]

2. On Information Privacy Suits More Generally

Beyond BIPA litigation in federal courts, a ruling settling the circuit split on standing under the Act would have implications for suits brought under other privacy laws that grant consumers a statutory right to sue violators.[292] This involves a broader circuit split regarding standing to sue for procedural statutory violations where the alleged injury is a future risk of harm.[293]

The Sixth and Ninth Circuits have held that the risk of future misuse of personal data can constitute a concrete harm sufficient to create standing. The Ninth Circuit articulated this in the *Patel* decision. The Sixth Circuit reached a similar conclusion in *Galaria v. Nationwide Mutual Insurance Company*, a suit brought under the FCRA.[294] There, the court found standing because of an

290. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1207 (Ill. 2019).

291. *Id.* at 1206.

292. Commentators have noted that since *Spokeo*, the Court has "remain[ed] reluctant to address privacy harms under Article III standing," denying certiorari to a number of cases involving Article III standing. Boyd Garriott & Megan Brown, *Zappos and the Supreme Court's Reluctance to Address Privacy Harms Under Article III Standing*, WILEY CONNECT (Mar. 27, 2019), https://www.wileyconnect.com/home/2019/3/27/zappos-and-the-supreme-courts-reluctance-to-address-privacy-harms-under-article-iii-standing [https://perma.cc/M27D-9YNR]. In fact, Circuit Judge Hamilton of the Seventh Circuit, in a concurring opinion to *Thornley*, implored the Supreme Court to "revisit the problem of standing in private actions based on intangible injuries under a host of federal consumer protection statutes." Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1251 (7th Cir. 2021) (Hamilton, J., concurring).

293. Facebook, the *Patel* defendant, discussed this split in its appeal to the Supreme Court, which was ultimately denied. *See* Petition for a Writ of Certiorari, *supra* note 189, at 21.

294. 663 F. App'x. 384, 385–86 (6th Cir. 2016).

"increased risk of fraud and identify theft" that resulted because the plaintiffs' data was part of a breach at the defendant insurance company.[295] The court did not require the plaintiffs to show their data was either actually misused or at an imminent risk of being misused as a result of the breach.[296]

Other circuits have ruled differently, holding that mere potential misuse of personal information is not sufficient to establish standing. In *Katz v. Pershing, LLC*, a Massachusetts consumer brought suit against a financial technology company, alleging their digital financial platform (of which the plaintiff was a user) failed to adequately protect user information in violation of the Massachusetts Unfair and Deceptive Trade Practices Act and the state's general consumer protection statutes.[297] Because "the plaintiff [did] not allege that her nonpublic personal information actually has been accessed by any unauthorized person," the First Circuit reasoned that the plaintiff's "cause of action rests entirely on the hypothesis that at some point an unauthorized, as-yet unidentified, third party might access her data and then attempt to purloin her identity."[298] Because the risk of harm the plaintiff alleged was "unanchored to any actual incident of data breach," the court held the plaintiff failed to "satisfy Article III's requirement of actual or impending injury."[299]

The Third Circuit reached a similar conclusion in *Reilly v. Ceridian Corp.*[300] There, the plaintiffs sued the defendant payroll processing company after the company suffered a breach in which a hacker infiltrated its systems and potentially gained access to personal and financial information belonging to about 27,000 people, though it was unknown whether the hacker read or copied that information.[301] The court held that the plaintiffs' "allegations of hypothetical, future injury are insufficient to establish standing" because the allegations relied on "speculation" that the hacker copied and intended to misuse their personal information.[302] Noting that "unless and until these conjectures come true, [plaintiffs] have not suffered any injury," the court dismissed the suit.[303]

Finally, like the First and Third Circuits, the Fourth Circuit also declined to find standing based upon future risk of data use in *Beck v. McDonald*, which involved a breach of medical information.[304] There, similar to *Reilly*, the court

295. *Id.* at 388.
296. *Id.*
297. 672 F.3d 64, 69–70 (1st Cir. 2012).
298. *Id.* at 79.
299. *Id.* at 80.
300. 664 F.3d 38, 42 (3d Cir. 2011).
301. *Id.* at 40.
302. *Id.* at 42.
303. *Id.* at 42, 46.
304. 848 F.3d 262, 267 (4th Cir. 2017).

held that the plaintiffs' allegation of an "enhanced risk" of identity theft was too speculative to establish standing.[305]

The resolution by the Supreme Court in the BIPA matter would also resolve this broader split, assuming the facts allege only a risk of misuse of the plaintiffs' biometric information that the procedural BIPA violation causes. Given the prevalence of data breaches and consumer discomfort with the use of personal information by private companies, a resolution finding standing for procedural violations is the right finding for this broader split as well because it provides consumers the ability to enforce their rights under the limited existing privacy statutes that allow them to do so, while incentivizing companies to highly prioritize compliance with existing regulations.

C. The Need for a More Permissive Understanding of Standing in the Context of Privacy

The correct reading of BIPA is that its provisions were established to protect individuals' concrete interests in the privacy of their biometric data: the law's provisions are not mere procedural rights, and even procedural or technical violations of the Act cause actual harm by depriving individuals of the privacy and control that BIPA was enacted to provide. It seems that the Illinois Legislature's intent in passing BIPA was not only to regulate the use of consumer biometric information, but to ensure they had a means to enforce such regulation *before* a data breach. This can be found in the legislative findings and intent section of the Act, which states that "biometrics are unlike other unique identifiers" because they are "unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[306] The Act compares biometrics, which are unchangeable, to other sensitive types of information such as Social Security numbers, which it notes "can be changed" when compromised.[307] This supports the finding that the intent of BIPA was not to merely regulate the use of biometric information, as the Second Circuit assumed, but to establish a right of privacy, at least from non-public entities, in one's biometric information.

This belief is further supported by other provisions of the Act's findings and intent section. BIPA notes that "an overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information."[308] The Act also states that "[t]he full ramifications of biometric technology are not fully known."[309] In addition to the

305. *Id.* at 274.
306. 740 ILL. COMP. STAT. 14/5(c) (2018).
307. *Id.*
308. *Id.* § 14/5(d).
309. *Id.* § 14/5(f).

provision, the final provision in the findings and intent section of BIPA states that "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric [data]."[310] Taking all of these provisions together, it would appear that the intent of the legislature was not merely to regulate the use of biometric data but to establish a right of privacy in it—i.e., to allow consumers to clearly choose which private entity they wished to allow to collect their biometric data and for what purpose.

The Act's substantive provisions clearly support this belief. They include strict provisions for consent: BIPA does not just require consent but requires a "written release executed by the subject of the biometric [data]" after the subject has been informed "in writing of the specific purpose and length of term for which . . . [the biometric data] is being collected, stored, and used" before the biometric data can be used.[311] It appears that the intent was to require companies to first provide written explanations of why they are collecting biometric data before receiving clear, written consent from consumers in order to proceed with the collection. This would support the belief that the intent behind BIPA was to establish a right of privacy in biometrics because consumers can clearly, under the Act, withhold their consent to the use of their biometrics if they find issue with the reasons why a company is using biometric information or to that company's length of retention of the biometrics.

With this more expansive reading of legislative intent, a procedural violation of BIPA constitutes a violation of the concrete privacy right that is behind the Act, not merely a procedural right, thus conferring standing under Article III. This is essentially what the Ninth Circuit held in *Patel*, stating that "[w]hen a private entity fails to adhere to the statutory procedures . . . the right of the individual to maintain his or her biometric privacy vanishes into thin air."[312] This is the correct interpretation and finding.

Furthermore, there is the practical matter of enforcement: the Act intended, unlike other state biometric privacy laws, to allow consumers the right to enforce their own right to privacy. That is made clear in the Act's provisions allowing "[a]ny person aggrieved by a violation" of BIPA to sue for liquidated damages of up to $5,000 per violation.[313] Especially in class action suits that can add up to actual and meaningful penalties (or, at least, large settlements) for companies that use biometrics, BIPA's monetary penalties may spur such companies to be

310. *Id.* § 14/5(g).

311. 740 ILL. COMP. STAT. 14/15(b)(2)-(3) (2018).

312. Patel v. Facebook, Inc., 932 F.3d 1264, 1274 (9th Cir. 2019) (citing Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1206 (Ill. 2019)).

313. 740 ILL. COMP. STAT. 14/20(1) (2018).

more careful in their biometric collection and use.[314] Furthermore, unlike other privacy statutes, the ability for consumers to bring suit means BIPA does not rely exclusively on state attorneys, who may be underfunded and overworked, for enforcement.

While there may be valid critiques for the ever-growing number of lawsuits filed in our litigious society, private litigation is recognized as a critical means of law enforcement in the American legal system, acting as an important supplement to public enforcement.[315] Scholars have noted that private actions allow individuals to "deal with problems that have not been adequately addressed by other institutions" and "[free] individuals from total dependence on collective bureaucratic remedies . . ."[316] Given the lack of robust data privacy regulations, combined with society's apparent desire for such regulations, this description sums up the role BIPA has played quite perfectly—it serves as a means for individuals to deal with problems surrounding data protection that the government has barely touched.

Further, given that private companies' use of biometrics are essentially unregulated outside of BIPA (and a few other state statutes),[317] and that the general public has a clear apprehension around both the use of biometric information and personal data generally,[318] tools like BIPA are needed to regulate the use of biometrics and personal information. The CCPA's inception in 2020, its expansion under the CPRA beginning in 2023, as well as the pending data privacy initiatives percolating in state legislatures across the country,[319] highlight society's desire for more regulation of the use of personal data. A finding by the Court that standing cannot exist for procedural violations would

314. Highlighting the fact that BIPA settlements can be of high enough financial importance to a company, Facebook's $550 million settlement of the Patel case was announced on its quarterly earnings call with investors in January 2020. Singer & Isaac, *supra* note 191.

315. J. Maria Glover, *The Structural Role of Private Enforcement Mechanisms in Public Law*, 53 WM. & MARY L. REV. 1137, 1143 (2012) (discussing "the American regulatory system's functional dependence on private regulation and the mechanisms that enable it").

316. Richard B. Stewart, *Crisis in Tort Law? The Institutional Perspective*, 54 UNIV. CHI. L. REV. 184, 198 (1987).

317. April Glaser, *Biometrics Are Coming, Along With Serious Security Concerns*, WIRED (Mar. 9, 2016, 11:00 AM), https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/ [https://perma.cc/YW9A-AV5T] (noting that "the use of data about [individuals'] body parts is largely unregulated").

318. A 2016 Deloitte study found that eighty-one percent of consumers feel they "have lost control over how their personal data are collected and used" by companies. Vikram Rao & Kruttika Dwivedi, *To Share or Not to Share: What Consumers Really Think About Sharing Their Personal Information*, DELOITTE INSIGHTS (Sept. 5, 2017), https://www2.deloitte.com/us/en/insights/industry/retail-distribution/sharing-personal-information-consumer-privacy-concerns.html [https://perma.cc/ZG4H-BHZN].

319. *See* Andrew Burt, *States are Leading the Way on Data Privacy*, THE HILL (Aug. 21, 2018, 10:30 AM), https://thehill.com/opinion/technology/402775-states-are-leading-the-way-on-data-privacy [https://perma.cc/66YH-UG3L].

ignore the headlines that consumers have seen for the past decade about the use of personal data and add to the public's apprehension surrounding private companies' use of their data. The multitude of data breaches[320] have left the impression that companies, left to their own devices, are unable to protect personal information effectively, and the disclosures of unauthorized, or at least less-than-forthcoming, collection and use of personal data by profit-making companies[321] leaves the impression they do not even care to try. A finding of Article III standing by the Supreme Court would update its standing jurisprudence to factor in our society's current understanding of the importance of data and privacy, and would not be out of left field, but instead build upon the Court's recent precedents—it has, after all, recently found that law enforcement's unrestricted use of new technologies can violate an individual's expectation of privacy.[322]

In the 21st century, where the use of personal information is worth billions of dollars or more[323] and consumers are left feeling helpless, procedural

320. *See, e.g.*, Tara Siegel Bernard et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html [https://perma.cc/3XTJ-42RQ]; Paul Ziobro & Danny Yadron, *Target Now Says 70 Million People Hit in Data Breach*, WALL ST. J. (Jan. 10, 2014), https://www.wsj.com/articles/no-headline-available-1389359240 [https://perma.cc/77J3-RNHN]; Kristina Libby, *100 Million Capital One Accounts Were Hacked in a Mass Data Breach*, YAHOO! (July 30, 2019), https://www.yahoo.com/lifestyle/100-million-capital-one-accounts-200200291.html [https://perma.cc/FC9J-A4CT]; Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS (Apr. 26, 2011, 6:56 PM), https://www.reuters.com/article/us-sony-stoldendata/sony-playstation-suffers-massive-data-breach-idUSTRE73P6WB20110427 [https://perma.cc/5DYJ-AY5Z].

321. *See, e.g.*, Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [https://perma.cc/9XDN-AGP3]; Jonathan Stempel, *Google faces $5 billion lawsuit in U.S. for tracking 'private' internet use*, REUTERS (June 2, 2020, 5:11 PM), https://www.reuters.com/article/us-alphabet-google-privacy-lawsuit-idUSKBN23933H [https://perma.cc/E93M-BXMW]; Kaya Yurieff, *Apple apologizes for listening to Siri recordings, promises changes*, CNN (Aug. 28, 2019, 3:11 PM), https://www.cnn.com/2019/08/28/tech/apple-siri-apology/index.html [https://perma.cc/LXQ4-6EST].

322. *See* Carpenter v. U.S., 138 S.Ct. 2206, 2209 (2018) (requiring the government to obtain a warrant supported before acquiring an individual's cell-site location information from wireless carriers).

323. There are a variety of estimates of the economic value of personal data to the global economy, many of which reach into the trillions of dollars. *See* Vasudha Thirani & Arvind Gupta, *The Value of Data*, WORLD ECONOMIC FORUM (Sept. 22, 2017), https://www.weforum.org/agenda/2017/09/the-value-of-data/ [https://perma.cc/EF3S-BBEK] (stating the value of the global data economy as three trillion dollars); HM TREASURY, THE ECONOMIC VALUE OF DATA: DISCUSSION PAPER 5 (2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf [https://perma.cc/GLP6-GD7K] (stating that "cross-border flows of data" were worth

violations of privacy regulations should be sufficient to constitute a concrete injury. It seems only fair that given the ability of companies to exploit consumer data for profit, that consumers should have the ability to enforce violations, even mere procedural ones, of their statutory rights in their data. The alternative leaves consumers the ability to enforce their privacy rights only after they have been violated and their information has leaked. The ineffectiveness of this situation is highlighted in the legislative intent provision of BIPA, which notes the inability of consumers to change their biometric information[324]—clearly, there should be a means to enforce violations of BIPA's protections before such violations result in a breach of immutable data. Given the significant settlements that BIPA has resulted in, and the fact that individual instances of biometric information collection may constitute individual violations, each worth $1,000 or $5,000 in liquidated damages, there are financial disincentives for companies to violate the Act's provisions.[325] Again, all of this is dependent on the ability to sue when these provisions are violated.

Standing for procedural violations additionally provides clarity for companies who use biometric information. Instead of performing a complicated analysis on whether a risk of injury can satisfy the concreteness requirement, standing would unify the federal courts with Illinois state courts and make clear that procedural violations provide a method for consumers to bring private actions, highlighting the importance of compliance.

$2.8 trillion, or 3.3% of global GDP, in 2014). The estimates of the data individual companies possess is also quite high; in the 2015 bankruptcy of Caesars Entertainment, its most valuable asset was determined to be the data it held on its customers who had joined its loyalty program, worth one billion dollars. *Fuel of the Future; The Data Economy*, THE ECONOMIST (May 6, 2017) (ProQuest, Doc. ID 1895923853). However, it is difficult to calculate the value of an individual firm's data in the absence of any accounting standards for valuation. *See generally* John Akred & Anjali Samani, *Your Data Is Worth More Than You Think*, MIT SLOAN MGMT. REV. (Jan. 18, 2018), https://sloanreview.mit.edu/article/your-data-is-worth-more-than-you-think/ [https://perma.cc/CW75-ERJA].

324. 740 ILL. COMP. STAT. 14/5(c) (2018).

325. The rising cost of BIPA noncompliance is even highlighted in marketing materials of companies selling compliance solutions and biometric technology. *See, e.g.*, *The Cost of BIPA Non Compliance is High*, GTB TECHNOLOGIES, https://gttb.com/cost-bipa-non-compliance-high/ [https://perma.cc/Y57Q-6K8M] (stating that "the cost of BIPA non-compliance is high" but that the company's Smart DLP product is "specifically designed to be able to demonstrate compliance of regulatory statutes"); *Biometrics: The Only Irrefutable Proof of Identity*, HID GLOBAL, https://www.hidglobal.com/solutions/biometric-regulations [https://perma.cc/5NCV-S36L] (stating that biometrics, which the company's technology products are designed to utilize, are "the simplest, most convenient and most secure way of proving identity" and that "addressing BIPA compliance requirements is well within the reach of most companies").

IV. CONCLUSION

While a federal data-privacy regulatory framework may be desirable,[326] a federal data law has not arrived and does not look likely given the current paralysis in Washington, D.C.[327] Thus, state privacy laws like BIPA stand on their own and should not be hamstrung by an outdated definition of standing that fails to account for the importance of personal information in today's society.[328] In fact, BIPA may be one of the most important data privacy regulations in the U.S. and is likely *the* most important biometric information law on the books, given its unique provision for private consumers to bring suit, its wide reach to defendants far outside of Illinois, and its potential for high financial penalties if individual instances of improper biometric collection or use constitute a separate violation. Commentators have noted that "only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses."[329] BIPA squarely gives consumers the right to enforce statutory violations involving their own biometric data, instead of leaving it up to state attorneys general, whose offices are subject to budgetary constraints and political pressure.[330]

326. Surprisingly, given the lack of movement on federal privacy regulation, essentially all stakeholders support the concept of federal privacy legislation. The national trade association for digital media and marketing businesses "strongly supports" a federal law. *IAB Urges Congress to Pass Federal Privacy Legislation to Protect Consumers & Avoid Patchwork of State Laws*, IAB (Feb. 26, 2019), https://www.iab.com/news/iab-urges-congress-to-pass-federal-privacy-legislation-to-protect-consumers-avoid-patchwork-of-state-laws/ [https://perma.cc/FRX5-NYUH]. Further, there is bipartisan support for a federal privacy law. Kate Kaye, *Cheat Sheet: What to Expect in State and Federal Privacy Regulation in 2021*, DIGIDAY (Feb. 1, 2021), https://digiday.com/media/cheatsheet-what-to-expect-in-state-and-federal-privacy-regulation-in-2021/ [https://perma.cc/2REX-C9YQ]. Oddly, the widespread support for such a law may work against its passage, because the devil, as always, is in the details: commentors note that while businesses want a uniform, national law with which to comply, they likely want this law to be weaker than the state laws currently on the books. *Id.* Further, Democrats and Republicans differ on several critical aspects of federal privacy regulation, including whether a federal law should override state and local laws, and whether the right to sue violators should be restricted to state attorneys general or extended to individuals. *Id.*

327. *See, e.g.*, John Hendel, *'Embarrassing': Congress Stumbles in Push for Consumer Privacy Bill*, POLITICO (July 12, 2019, 5:51 PM), https://www.politico.com/story/2019/07/12/congress-consumer-privacy-bill-1582540 [https://perma.cc/57DZ-FWBB].

328. If anything, more and more patchwork state laws may pressure the federal government into enacting federal privacy legislation. *See* Mark Smith, *Analysis: California Gamble Raises Odds on Federal Privacy Law*, BLOOMBERG LAW (July 2, 2020, 11:52 AM), https://www.bloomberglaw.com/product/privacy/document/XE6145DC000000 [https://perma.cc/A8HF-MF3C].

329. Hartzog, *supra* note 67, at 101.

330. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 797, 804 (2016).

The Seventh and Ninth Circuits were correct in finding that BIPA confers privacy rights in individuals' biometric information, and that the violation of these rights—the failure to adhere to BIPA's requirements—is sufficient to confer Article III standing. Given the clear intent behind the Illinois Legislature's passage of BIPA and the importance of protecting biometric information prior to its unauthorized disclosure, it is time for a new understanding of standing in privacy contexts that allows consumers to bring suit for privacy violations when statutes like BIPA give them the right to do so.

MICHAEL MCMAHON*

* J.D., 2021, Saint Louis University School of Law. I would like to thank Professor Matthew Bodie for his guidance on this article.