NOTE

Give Up Your Face, and a Leg to Stand on Too: Biometric Privacy Violations and Article III Standing

*Sojung Lee**

ABSTRACT

The standing doctrine says that a plaintiff only has standing when that plaintiff has suffered a concrete injury that is fairly traceable to the defendant, and the court can likely provide redress for the injury. The doctrine becomes complicated when addressing instances of privacy harms because these harms are usually intangible and sometimes speculative. This is especially true for cases of biometric privacy, where the alleged harm comes from a violation of a biometric privacy statute regulating the collection, use, and storage of a person's biometric data. There has been division among the courts as to whether such a statutory violation amounts to a concrete injury sufficient for Article III standing. This Note argues that, after the decision in TransUnion v. Ramirez*, courts should apply* Ramirez *to allow standing in biometric privacy suits. To read* Ramirez *otherwise would lead to an absurd result and a usurpation of legislative determinations. Therefore, in order to respect legislative intent and protect people's privacy interests, this Note argues that courts should allow Article III standing in instances of biometric privacy statutory violations.*

* J.D., May 2022, The George Washington University Law School.

Table of Contents

Introduction

Privacy data in the form of biometric identifiers is valuable in a technology age with substantial data collection by businesses. Clearview AI, Inc., a small company in New York, used a technique called screen scraping[1] to collect around three billion images of peoples' faces across platforms such as Google, Facebook, Venmo, and YouTube, and create a massive facial recognition database.[2] The company offers a service that enables any user to upload a picture of an individual, view public photos of that person, and even provide the

1 "Screen scraping is the process of collecting screen display data from one application and translating it so that another application can display it." *Screen Scraping*, Techopedia, https://www.techopedia.com/definition/16597/screen-scraping [https://perma.cc/SR39-QNHH].

2 Katherine Soule, *Facial Recognition: A Clear View to Dystopia*, JDSupra (May 13, 2020), https://www.jdsupra.com/legalnews/facial-recognition-a-clear-view-to-22273/ [https://perma.cc/2DZ7-FUTH].

links to those photos.[3] This service not only sounds like a rather convenient gift for potential stalkers, but is also now a tool in the hands of hundreds of law enforcement agencies, including the Federal Bureau of Investigation and the Department of Homeland Security.[4] It can be used to find activists at social protests, or someone who decided to "Like" a certain page on Facebook, "revealing not just their names but where they lived, what they did and whom they knew."[5]

There are several uneasy implications in this situation. One is the potential misuse or misapplication of technology toward the general public—especially if data breaches place the data in the possession of more sinister third parties. Another is the ease with which billions of pictures of people were collected and cataloged without their permission or knowledge of what the photos were being used for.[6] Following a data breach in early 2020, Clearview, the tiny startup that now wields so much power in biometric information, reassured the public by stating that "[u]nfortunately, data breaches are part of life in the 21st Century."[7]

Data used for facial recognition falls into a class of unique physical, behavioral, or biological characteristics called biometrics.[8] Biometric data includes fingerprints, face and iris scans, keystroke dynamics, and even the way someone walks.[9] Biometric data is unique in that an individual's biometric identifiers generally cannot be replaced if compromised.[10] A password, PIN number, and credit card are easily replaceable if compromised. But in the advent of facial recognition, fingerprinting, and iris scans for identification and security purposes, an individual's facial features, an index fingerprint, or an eyeball cannot be reissued at all.[11]

---

3 Kashmir Hill, *The Secretive Company that Might End Privacy as We Know It*, N.Y. Times (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/8RGJ-HMNG] (describing Clearview as a "tool that could end your ability to walk down the street anonymously").

4 *Id.*

5 *Id.*

6 *Id.*

7 *Clearview AI: Face-collecting Company Database Hacked*, BBC News (Feb. 27, 2020), https://www.bbc.com/news/technology-51658111 [https://perma.cc/QQ82-7HHG].

8 *Biometrics*, U.S. Dep't of Homeland Sec. (Dec. 14, 2021), https://www.dhs.gov/biometrics [https://perma.cc/2YGE-5ZBV].

9 World Bank, *Biometric Data*, *in* Practicioner's Guide 122–28 (2019), https://id4d.worldbank.org/guide/biometric-data [https://perma.cc/DS3J-96HD].

10 *Id.*

11 *Id.*

There is no federal law in the United States that regulates biometric data yet.[12] Privacy law in the United States has taken a sectoral approach, with some federal laws such as the Health Insurance Portability and Accountability Act of 1996 ("HIPPA")[13] and the Gramm-Leach-Bliley Act[14] directed only to specific industries. Some states have already passed protective measures restricting the collection and use of biometric data, particularly due to the increasing use of biometric information and the potential for its misuse.[15] State legislation accomplishes this regulation either through a biometric privacy law or a general data privacy law, which defines biometric data as an area for protection.[16] A prominent example of a biometric privacy law is Illinois's Biometric Information Privacy Act ("BIPA"),[17] which regulates the collection and use of biometric data.[18] Because there is not yet a federal statute regulating biometric information, cases involving biometric privacy issues do not arise on the first instance based on a federal statute, but on state statutes.[19] As privacy is a significant and current issue, discussions about privacy will likely continue to expand as a major focus point for legislatures going forward.[20]

A common trend shows that biometric privacy cases are usually brought in state court, removed to federal court by defendants,[21] and

---

12 *The Proliferation of Biometric Data and Legislation to Regulate its Use*, TANNENBAUM HELPERN SYRACUSE & HIRSCHTRITT LLP, https://www.thsh.com/publications/the-proliferation-of-biometric-data-and-legislation-to-regulate-its-use [https://perma.cc/S9H2-WSNR].

13 Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 26 U.S.C., 29 U.S.C., 42 U.S.C.). Among other things, this act regulates the storage of medical information. *Id.* §§ 261–264, 110 Stat. 1936, 2021–34 (codified at 42 U.S.C. § 1320d).

14 Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 U.S.C., 15 U.S.C.). Among other things, this act regulates financial institutions in safeguarding sensitive data. *Id.* §§ 501–510, 113 Stat. 1338, 1436–45 (codified at 15 U.S.C. §§ 6801–6809).

15 Kristine Argentine & Paul Yovanic, *The Growing Number of Biometric Privacy Laws and the Post-COVID Consumer Class Action Risks for Businesses*, JDSUPRA (June 9, 2020), https://www.jdsupra.com/legalnews/the-growing-number-of-biometric-privacy-62648/ [https://perma.cc/3CV5-7YFP].

16 As of 2020, eight states have passed laws regulating biometric information, and another eleven have at least proposed biometric privacy legislation within the past decade. *Id.*

17 740 ILL. COMP. STAT. 14 (2021).

18 Argentine & Yovanic, *supra* note 15.

19 In particular, the Illinois Biometric Privacy Act has a private right of action for recovering statutory damages when defendants do not comply with the statute. *See id.*; *see infra* Part I.

20 *See Senators Seek Limits on Biometric Data Collection*, IDENTITY WEEK (Aug. 6, 2020), https://identityweek.net/senators-seek-limits-on-biometric-data-collection/ [https://perma.cc/F6RH-CPG8]. In 2020, U.S. Senator Jeff Merkley introduced a national biometric privacy law with Senator Bernie Sanders. *Id.* Other pieces of legislation will likely be considered and proposed while concerns about privacy continue to grow.

21 *See, e.g.*, Hilliard v. Panera, LLC, No. 1:21-cv-00233 (N.D. Ill. Jan 14, 2021); Brewton v. First Student, Inc., No.1:20-cv-07017 (N.D. Ill. Nov 25, 2020).

then dismissed for lack of Article III standing.[22] Article III standing is a doctrine that describes the ability of a party to have the right to bring a lawsuit to the federal courts.[23] The lack of standing will cause the case to be dismissed and the court will not hear the lawsuit.[24] The Supreme Court created a three-part test for the standing doctrine, and the first part involves finding an injury-in-fact that is "concrete and particularized" and "actual or imminent."[25] When a biometric privacy suit reaches a federal court, however, there has been a lack of general consensus among the federal courts over whether a plaintiff suing for biometric privacy violations has a sufficiently "concrete and particularized" injury to sustain Article III standing.[26]

The Second Circuit and the Ninth Circuit have ruled in direct opposition with each other on this matter, creating a circuit split.[27] The point of dispute is whether or not plaintiffs have alleged a concrete and cognizable injury when plaintiffs only allege violations of a statutory procedural right.[28] While the Second Circuit has found no concrete injury—and thus, no standing—when companies are not complying with biometric privacy statutes,[29] the Ninth Circuit recognizes such procedural violations as sufficiently concrete injuries for standing.[30]

Most recently, the Supreme Court found no injury for procedural violations of the Fair Credit Reporting Act of 1970 ("FCRA")[31] in *TransUnion LLC v. Ramirez*,[32] but it is yet to be seen how this decision will be applied to cases in federal court concerning biometric information. As the Supreme Court has declined to grant review on whether procedural violations of state biometric privacy statutes constitute an injury,[33] the situation remains unclear for potential litigants.

---

22 *See* Hazlitt v. Apple Inc., 500 F. Supp. 3d 738 (S.D. Ill. 2020), *vacated sub nom. In re* Apple Inc., No. 20-8033, 2021 WL 2451296 (7th Cir. Jan. 22, 2021).

23 Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992).

24 *See id.*

25 *Id.*

26 Greg Margolis & Jane Metcalf, *What You Do Know Can't Hurt You: Standing and the Illinois Biometric Privacy Act*, PATTERSON BELKNAP (Sept. 2, 2020), https://www.pbwt.com/misbranded/what-you-do-know-cant-hurt-you-standing-and-the-illinois-biometric-privacy-act/ [https://perma.cc/PU99-XHCV].

27 *See id.*

28 *Compare* Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 15 (2d Cir. 2017), *with* Patel v. Facebook, Inc., 932 F.3d 1264, 1270 (9th Cir. 2019).

29 *See Santana*, 717 F. App'x at 15.

30 *See Patel*, 932 F.3d at 1270.

31 Pub. L. No. 91-508, 84 Stat. 1128 (1970) (codified at 15 U.S.C. § 1681).

32 141 S. Ct. 2190, 2207–14 (2021).

33 *Supreme Court Leaves the Door Open for Expansive Biometric Privacy Lawsuits*,

This leaves room for confusion for private entities collecting, using, and storing biometric information because of the inconsistent application of the law.

This Note argues that federal courts should apply *Ramirez* to allow standing in cases involving biometric data collection or usage, thus following the Ninth Circuit's model for biometric privacy cases, because biometric privacy violations are sensitive and permanent in nature. More specifically, federal courts should not apply *Ramirez* literally in lawsuits alleging biometric privacy violations because literal application would lead to the absurd results of denying standing for countless longstanding statutes, under deterrence, stagnation in the law, and a usurpation of the legislative branch. Allowing plaintiffs to litigate in federal court will recognize and protect the sensitivity of their biometric information by keeping companies handling this data, like Clearview, under scrutiny and accountable for their actions.

Part I of this Note gives a brief overview of standing under *Spokeo, Inc. v. Robins* ("*Spokeo I*")[34] and the implications of *Ramirez* on the standing doctrine. Part II describes the positions of the Ninth, Second, and Seventh Circuits on the issue of statutory violations and standing in biometric privacy cases, detailing the landmark cases and each court's rationale for its stance. Part III argues that federal courts should apply *Ramirez* to allow Article III standing in instances of biometric privacy violations and should not read the *Ramirez* holding literally because that would only lead to illogical outcomes.

I. Background

Article III of the Constitution provides the basis for the standing doctrine by mandating that judicial power only extend to cases and controversies.[35] The Supreme Court developed judicial standing through case law to ensure both that federal courts do not go beyond their traditional authorities and that the category of litigants to file suit in federal court is properly limited.[36] Standing requires that (1) the plaintiff has suffered an injury-in-fact, (2) which is fairly traceable to the alleged conduct, and (3) is likely to be redressed by a favorable judicial decision.[37] The first factor is the heart of the issue

---

O'Melveny & Myers LLP (Jan. 23, 2020), https://www.omm.com/resources/alerts-and-publications/alerts/supreme-court-leaves-the-door-open-for-expansive-biometric-privacy-lawsuits/ [https://perma.cc/MP3W-HMT7].

34 578 U.S. 330 (2016).

35 U.S. Const. art. III, § 2.

36 *See Spokeo I*, 578 U.S. at 337–38.

37 Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992).

for alleged biometric privacy violations and whether there is sufficient Article III standing, and therefore this Note will consider only the first factor in more detail. In particular, biometric privacy claims under the private right of action granted by the Biometric Information Privacy Act, have faced significant barriers in court over whether plaintiffs have suffered an actual, concrete injury sufficient to pursue litigation.[38]

A. Spokeo*,* Ramirez*, and the "Injury-in-fact" Requirement*

For years, the Supreme Court offered guidelines for deciding what constitutes an "injury-in-fact" without setting forth a clear rule, leaving lower courts struggling to interpret its meaning.[39] In *Spokeo*, the Supreme Court was presented with the question of whether a plaintiff suing under the FCRA had sufficient standing to bring an action in federal court when there was a willful violation of the FCRA absent actual harm or claim of damages.[40] The Supreme Court remanded to the lower court without deciding the standing issue.[41] The Court stated, however, that even in cases of statutory violations, Article III standing required a concrete injury.[42] Although intangible injuries could be considered concrete, the Court held that the injury-in-fact requirement was not automatically fulfilled whenever a statute articulated a statutory right with means to sue for violations of that right.[43] At the same time, the Court also stated that it was possible for a violation of a procedural right itself to be sufficient, and additional harm did not need to be shown to prove injury-in-fact.[44] The Court left it to the lower courts to decide under which circumstances a mere statutory violation was enough to clear the standing hurdle.[45] The flexible standard set in *Spokeo* left lower courts trying to interpret and apply *Spokeo*'s concrete injury requirement for Article III standing, often leading to inconsistent applications of the *Spokeo* decision between courts.[46]

---

38 *See infra* Section I.B.

39 *See Spokeo I*, 578 U.S. at 339–43; *see also* Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 473 (1982).

40 *Spokeo I*, 578 U.S. at 333–35.

41 *Id.* at 334–35.

42 *Id.* at 341 (holding that plaintiff "could not . . . allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III").

43 *Id.* at 342–44.

44 *Id.* at 340–44.

45 *Id.* at 342–44.

46 *See, e.g.*, Gadelhak v. AT&T Servs., Inc., 950 F.3d 458, 463 & n.2 (7th Cir. 2020) (finding any unwanted text message caused a concrete injury for purposes of standing after applying

Recently, the Supreme Court offered a bit of clarity with its 5–4 decision in *Ramirez*, when the Court revisited the situation of inaccurate credit reports and requirements for Article III standing.[47] In *Ramirez*, TransUnion issued a report that identified the plaintiff, Ramirez, as a potential terrorist simply because he shared a first and last name with an individual on the government's terrorist watch list.[48] After a dealership refused to sell him a car, Ramirez filed a class action suit on behalf of himself and thousands of other people who had also been incorrectly identified.[49] Although the Court decided that Ramirez had suffered a concrete injury, it held that only those who, like Ramirez, also had this information disseminated to third parties had a claim, while the rest who had merely been misidentified as a terrorist did not.[50] Thus, in *Ramirez*, the majority clarified that a plaintiff in a class action claiming a mere statutory violation does not have standing and therefore cannot win statutory damages, even if that violation would otherwise entitle them to statutory damages.[51] One dissent in this 5–4 decision was quick to point out that this was an unacceptable assertion of control by the judiciary over the legislature by noting that "never before [had the] Court declared that legislatures are constitutionally precluded from creating legal rights enforceable in federal court" if the rights were not grounded historically or at common law.[52]

The question of whether or not there was a concrete injury has always been at the forefront of many information privacy and security claims. In many cases of alleged privacy violations, plaintiffs have their data compromised, but courts are often reluctant to recognize a cognizable injury with just the acquisition of data because courts traditionally view harm as something both current and materialized.[53] The decision in *Ramirez* reinforces this notion. Privacy claims become more unclear if the data or information involved has not yet been

Spokeo); Salcedo v. Hanna, 936 F.3d 1162, 1173 (11th Cir. 2019) (finding that single unwanted text message did not result in type of harm that constitutes injury-in-fact for purposes of standing).

47 TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021).

48 *Id.* at 2201.

49 *Id.* at 2201–02.

50 *Id.* at 2207–14.

51 *Id.* at 2205–14.

52 *Id.* at 2221 (Thomas, J., dissenting).

53 *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 754 (2018) (arguing that courts are overly narrow in insisting data breach harms be both "visceral" and "vested" before harm is recognized).

inappropriately used or disseminated to third parties.[54] Different interpretations by federal courts before *Ramirez* led to a circuit split on the issue of standing and biometric privacy violations.[55] After *Ramirez*, the courts will be a testing ground for the newly articulated standing concepts.[56]

The judicial branch, however, has generally been slow to address the severe privacy issues that come with modern advancements in technology and biometrics.[57] The lack of a strong legal framework and judicial safeguards regarding biometric data is leading to mass privacy violations.[58] Biometric data will continue to be a major modern privacy concern for privacy experts, domestic and international legislatures,[59] and litigants in federal courts despite *Ramirez*. As federal courts begin to grapple with *Ramirez* and continue wrestling with how to handle biometric data and its unique sensitivities, this Note recommends that federal courts distinguish *Ramirez* from the biometric data context.

B. Biometric Privacy Claims Under BIPA

As technologies continue to advance, biometric data has become an invaluable source of information to many businesses.[60] The role and application of biometric information is increasingly expanding throughout various industries in the world, from law enforcement to businesses, for purposes of security, identification, and authentica-

---

54 Priscilla Fasoro & Lauren Wiseman, *Standing Issues in Data Breach Litigation: An Overview*, COVINGTON & BURLING LLP (2018), https://www.insideprivacy.com/data-security/data-breaches/standing-issues-in-data-breach-litigation-an-overview [https://perma.cc/23E8-Y44K].

55 *See infra* Part II.

56 Abby L. Risner & Lauren A. Daming, *SCOTUS Decision in* TransUnion LLC v. Ramirez *Raises Hurdle for Establishing Standing in Class Action Claims Under the Illinois Biometric Information Privacy Act and Other Data Privacy and Consumer Protection Statutes*, WESTLAW TODAY (July 13, 2021), https://www.greensfelder.com/media/publication/583_Risner_Daming_Westlaw%20Today.pdf [https://perma.cc/S8EF-3WB2].

57 *See* Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/2014/04/15/172377/laws-and-ethics-cant-keep-pace-with-technology/ [https://perma.cc/AR92-2448].

58 *See* Jennifer Lynch & Adam Schwartz, *Victory! Illinois Supreme Court Protects Biometric Privacy*, ELEC. FRONTIER FOUND. (Jan. 25, 2019), https://www.eff.org/deeplinks/2019/01/victory-illinois-supreme-court-protects-biometric-privacy [https://perma.cc/Q2FS-Y3WU].

59 *See* Danny Ross, *Processing Biometric Data? Be Careful, Under the GDPR*, IAPP (Oct. 31, 2017), https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/ [https://perma.cc/M9PP-WNA7] ("GDPR specifically singles out biometric data as a 'sensitive' category of personal information, warranting robust protection.").

60 *See* Elizabeth M. Walker, *Biometric Boom: How the Private Sector Commodifies Human Characteristics*, 25 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 831, 834–35 (2015).

tion.[61] Because biometric identifiers are unique in nature, they are regarded by companies to be secure, convenient, and more reliable data for identification and security purposes.[62] The use of biometric identifiers are therefore likely to become even more prevalent in the future.[63] But the potential misuse and risks apparent from this trajectory have rightfully raised concerns about security and privacy rights.[64]

In response, some states have proposed and passed legislation that sets the framework for the collection, retention, and destruction of biometric data by private entities.[65] Illinois's BIPA has been at the forefront of biometric privacy regulations because it is the oldest and most comprehensive biometric privacy law in the United States.[66] Because there are few laws governing biometric data that exist in the United States,[67] many other states are attempting to implement, or are in the process of implementing, similar legislation to BIPA, following a current movement towards state regulation of biometric information.[68] Before 2018, only Illinois, Texas, and Washington had biometric privacy laws.[69] Within a year, the number almost tripled.[70] BIPA still remains particularly relevant to the plaintiffs' bar because until recently it was the only statute that regulated biometric privacy and included a private right of action for any Illinois resident "aggrieved" by a violation of the Act.[71] California's Consumer Privacy Act of 2018

---

61 Examples include facial recognition used by casinos to identify known card counters and corporations using heartbeats to authenticate employees. Jayshree Pandya, *Hacking Our Identity: The Emerging Threats from Biometric Technology*, FORBES (Mar. 9, 2019, 12:26 PM), https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology/ [https://perma.cc/9PHH-XVQT].

62 *See The Proliferation of Biometric Data and Legislation to Regulate its Use*, *supra* note 12.

63 *Id.*

64 *Biometric Security Poses Huge Privacy Risks*, SCI. AM. (Jan. 1, 2014), https://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks/ [https://perma.cc/A8HR-LSFK].

65 Soule, *supra* note 2.

66 *See* 740 ILL. COMP. STAT. 14/5(e) (2021); Christopher Ward & Kelsey C. Boehm, *Developments in Biometric Information Privacy Laws*, FOLEY & LARDNER LLP (June 17, 2021), https://www.foley.com/en/insights/publications/2021/06/developments-biometric-information-privacy-laws [https://perma.cc/8HX8-TVYM].

67 In Europe, the General Data Protection Regulation ("GDPR") also regulates biometric data and defines the term quite broadly. *See The Proliferation of Biometric Data and Legislation to Regulate its Use*, *supra* note 12; Argentine & Yovanic, *supra* note 15.

68 Arkansas, California, Texas, and Washington are four states that have developed legislation modeled on BIPA. Ward & Boehm, *supra* note 66.

69 Argentine & Yovanic, *supra* note 15.

70 *Id.*

71 740 ILL. COMP. STAT. 14/20 (2021).

("CCPA")[72] identifies "personal information" beyond biometric identifiers while also providing for a private right of action, though consumers can only sue if their information is accessed or disseminated without authorization.[73] While BIPA does not prohibit the collection of biometric data itself, the act demands certain affirmative obligations from the private entities that choose to do business within Illinois,[74] including notice and written consent from the individual whose biometric data is being collected.[75] Importantly, BIPA's private right of action provides any Illinois resident "aggrieved by a violation" of the statute the right to sue and seek damages for violations of its provisions, ranging from $1,000 up to $5,000 for reckless or intentional violations.[76]

BIPA litigation has been on the rise for consumer class actions across the United States because of the statute's broader scope compared with other state biometric privacy statutes, and the possibility of statutory damages.[77] In many cases, the defendant will remove the case to federal court under diversity of citizenship jurisdiction, and then move to dismiss for lack of Article III standing.[78] In 2020, how-

---

72 CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2020).

73 *Id.* §§ 1798.140, 1798.150. The CCPA's application to businesses and its employees began in January 2020 and will surely continue to shape the legal landscape of biometric privacy claims. *See The Proliferation of Biometric Data and Legislation to Regulate its Use*, *supra* note 12.

74 The issue of personal jurisdiction is a separate issue, and one that can make it difficult for Illinois residents to bring suit in Illinois when a national company is headquartered in a different state. Plaintiffs, however, are still able to sue these companies for BIPA violations in other states, including the companies' home states. *See* Joshua Fattal, David Kantrowitz & Natalie Perez, *Recent Decisions in Illinois Limit BIPA's Reach, but California Begs to Differ*, JDSUPRA (Mar. 8, 2021), https://www.jdsupra.com/legalnews/recent-decisions-in-illinois-limit-bipa-9126655/ [https://perma.cc/C9R7-MUGD].

75 Monica R. Chmielewski, Samuel D. Goldstick, Aaron K. Tantleff, John L. Litchfield & Patrick J. McMahon, *Biometric Privacy: Illinois Supreme Court Decision Allows Claims to Proceed Without Showing of Actual Harm*, FOLEY & LARDNER LLP (Feb. 4, 2019), https://www.foley.com/en/insights/publications/2019/02/biometric-privacy—illinois-supreme-court-decision [https://perma.cc/4YE8-4DAC].

76 740 ILL. COMP. STAT. 14/20 (2021).

77 *See* Rochelle Swartz & David T. Cohen, Rivera v. Google *Bolsters Article III Challenges to Privacy Suits - but Risks Remain*, ORRICK HERRINGTON & SUTCLIFFE LLP (Jan. 24, 2019), https://blogs.orrick.com/trustanchor/2019/01/23/rivera-v-google-bolsters-article-iii-challenges-to-privacy-suits-but-risks-remain/ [https://perma.cc/47BH-LDHK].

78 *See, e.g.*, Hazlitt v. Apple Inc., 500 F. Supp. 3d 738 (S.D. Ill. 2020), *vacated sub nom. In re* Apple Inc., No. 20-8033, 2021 WL 2451296 (7th Cir. Jan. 22, 2021) (vacated and remanded to reconsider in light of subsequent decisions); Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 620 (7th Cir. 2020). A review of Illinois dockets over a three-month period showed that thirty-six of forty-eight BIPA complaints were removed from state court, revealing the frequency of this occurrence. Jennifer Marsh, *Analysis: 7th Circuit's BIPA Rulings Provide State Court Roadmap*, BLOOMBERG L. (Feb. 18, 2021, 11:46 AM), https://news.bloomberglaw.com/tech-and-telecom-

ever, BIPA filings in federal courts brought by plaintiffs significantly increased as well under diversity jurisdiction, following new case law that clarified Article III standing requirements for biometric privacy suits.[79] The circuit split therefore directly influences the choice in forum available to litigants, as well as whether a case will be heard or dismissed before reaching the merits.[80] While *Ramirez* sheds some light on the choice of forum issue, the decision does not stop forum shopping in biometric privacy cases because *Ramirez* does not resolve the standing question within the biometric space. Individuals might still choose the circuit that they believe will lead to a favorable outcome, looking to previous BIPA decisions and the courts' application of *Spokeo*.

Lawsuits under BIPA often may concern failure to provide written notice about the details of the collection of their biometric information, or failure to obtain written consent,[81] under section 15(b).[82] Additionally, under section 15(a), some plaintiffs may allege injury through violation of the written policy requirement, which states that entities must publicly provide a written policy for the retention period and subsequent destruction of the biometric data they were collecting and storing.[83] At times, the claim also may involve section 15(c), which forbids private entities from selling, trading, or profiting from some-

law/analysis-7th-circuits-bipa-rulings-provide-state-court-roadmap [https://perma.cc/2RB8-GCML].

79 The landmark decision by the Illinois Supreme Court finding standing for plaintiffs for a violation of BIPA without "actual injury" opened the door for BIPA litigation and further discussions about Article III standing in federal court. *See infra* Section II.A.1. Federal complaints alleging BIPA claims more than doubled from 2018 to 2019 and had already almost doubled again by mid-2020. Jennifer Marsh, *Analysis: Biometrics Privacy Class Actions Increase This Year*, BLOOMBERG L. (Nov. 6, 2020, 4:18 AM), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-biometrics-privacy-class-actions-increase-this-year [https://perma.cc/SZG4-WS2E]. The increase in BIPA complaints continued until 2021, after which the amount of BIPA complaints remained relatively steady. Kristin L. Bryan, Christina Lamoureux & Dan Lonergan, *2021 Year in Review: Biometric and AI Litigation*, NAT'L L. REV. (Jan. 5, 2022), https://www.natlawreview.com/article/2021-year-review-biometric-and-ai-litigation [https://perma.cc/3ASY-78Y4].

80 *See* Risner & Daming, *supra* note 56.

81 A current bill being considered by the Illinois General Assembly that would change BIPA's language from "written release," to "consent" including through "electronic means," suggests that currently the "written" consent requirement under BIPA would not be satisfied through electronic agreement. *See* Grace Barbic, *Lawmakers Revisit Data Collection Privacy Laws*, CAPITOL NEWS ILL. (Mar. 10, 2021), https://capitolnewsillinois.com/NEWS/lawmakers-revisit-data-collection-privacy-laws [https://perma.cc/CN65-TANT].

82 740 ILL. COMP. STAT. 14/15(b) (2021).

83 *Id.* 14/15(a).

one's biometric identifiers.[84] Whether these plaintiffs are sufficiently "aggrieved by a violation" in these instances to have Article III standing to bring BIPA suits in federal court has been an imperative question for courts.

II. Current Interpretation of the Standing Doctrine in Biometric Privacy Litigation

The federal courts have yet to fully consider *Ramirez*'s reluctance to acknowledge statutory violations as concrete injuries. Thus, the *Spokeo* decision still provides the main guideposts for different circuits to come up with their own approach towards Article III standing within the biometric space. This Part explores how, under *Spokeo*, the question of whether a procedural violation of BIPA causes concrete injury sufficient for Article III standing has resulted in a circuit split among the Ninth, Second, and Seventh Circuits. Section A describes the Ninth Circuit's holding that violations of BIPA inflicted harm on plaintiffs by denying their common law right to privacy, which fulfilled the standing requirement. Section B details the Second Circuit's holding that a mere procedural violation of BIPA did not result in a concrete injury that satisfied Article III standing. Section C explains that the Seventh Circuit mainly agreed with the Ninth Circuit in finding a violation of personal rights, which constituted a concrete and particularized injury that satisfied Article III standing, though the court distinguished between the different sections of BIPA.

A. The Ninth Circuit's Application of the Law

The Ninth Circuit has found sufficient injury and Article III standing where there have been violations of concrete privacy interests protected by statutory provisions.[85] On remand, the Ninth Circuit in *Robins v. Spokeo, Inc.* ("*Spokeo II*")[86] found that the harm requirement of *Spokeo* depended on whether the statutory provisions were implemented to protect the plaintiff's concrete rights, and whether violations alleged actually harmed, or resulted in a material risk of harm, to those interests.[87] In this case, Robins claimed that a company, Spokeo, willfully violated a statutory provision by publishing false information about him on its website.[88] Using the harm require-

84 *Id.* 14/15(c).

85 *See* Campbell v. Facebook, Inc., 951 F.3d 1106, 1119 (9th Cir. 2020).

86 867 F.3d 1108 (9th Cir. 2017).

87 *See id.* at 1110–11, 1117.

88 Spokeo, Inc. v. Robins (*Spokeo I*), 578 U.S. 330, 333 (2016).

ment interpretation, the Ninth Circuit held that the plaintiff still satisfied Article III's concrete harm requirement.[89] The rationale depended on the fact that the statutory provision in this case, the FCRA, was enacted by Congress to protect consumers from the dissemination of false information and inaccurate consumer reports.[90] The Court reasoned that these protections were related to privacy protections available at common law and served to protect the consumer's concrete rights, which could be harmed by incorrect credit reports.[91] The Ninth Circuit held that the FCRA violation caused sufficient injury to confer standing.[92]

1. Rosenbach v. Six Flags Entertainment Corp.

The reasoning that a procedural violation of biometric privacy constitutes harm sufficient for standing has its origins in state court. In *Rosenbach v. Six Flags Entertainment Corp.*,[93] a minor challenged an amusement park for collecting his thumb print without his informed consent, which is a requirement under BIPA.[94] The Illinois Supreme Court ruled that a plaintiff only needs to allege a violation of BIPA rather than actual harm to have a claim under the Act.[95] The court recognized that the legislature codified an individual's "right to privacy in and control over their biometric identifiers and biometric information," which was important due to the particularly sensitive and unique nature of biometric identifiers.[96] Because plaintiffs were "clearly . . . 'aggrieved'" by the BIPA violations, which took away their right to privacy and to control their own biometric information, the court found that the injury was "real and significant."[97] The *Rosenbach* decision led to hundreds of BIPA lawsuits filed in Illinois courts.[98] The *Rosenbach* ruling that a plaintiff could be aggrieved

89 *Spokeo II*, 867 F.3d at 1118.

90 *Id.* at 1113.

91 *Id.* at 1114–15.

92 *Id.* at 1117.

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

94 *Id.* at 1201–02.

95 *Id.* at 1201–02, 1207.

96 *Id.* at 1206 (finding that the moment there is a statutory violation, "the right of the individual to maintain [his or] her biometric privacy vanishes into thin air" (quoting Patel v. Facebook, Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018))).

97 *Id.*

98 Richard R. Winter, Rachel C. Agius & William F. Farley, *BIPA Update: Class Actions on the Rise in Illinois Courts*, HOLLAND & KNIGHT LLP (July 22, 2019), https://www.hklaw.com/en/insights/publications/2019/07/bipa-update-class-actions-on-the-rise-in-illinois-courts [https://perma.cc/NFR6-JYY7].

under BIPA without a concrete injury, combined with subsequent federal BIPA cases finding sufficient injury-in-fact for Article III standing in federal court, made it easier for plaintiffs to bring suit in federal court or allege BIPA class actions in general.[99]

2. Patel v. Facebook, Inc.

In 2019, the Ninth Circuit directly addressed the standing question in BIPA lawsuits when a class of Illinois plaintiffs sued the tech giant Facebook using *Rosenbach* as precedent.[100] In the landmark case *Patel v. Facebook, Inc.*,[101] a class action alleged violation of BIPA when Facebook scanned and identified users in uploaded pictures for its "Tag Suggestions" program, doing so without prior written notice or consent under Section 15(b), and without a compliant data retention schedule under Section 15(a).[102] Facebook argued that the plaintiffs were not "aggrieved" by BIPA violations and could not bring the action because there was no actual, tangible injury for Article III standing.[103]

The *Patel* court reached a decision that suggested that challenges to Article III standing for future BIPA litigation in federal court lacked viability.[104] Because BIPA is intended to protect peoples' concrete privacy interests by giving them certain rights over the collection, storage, and dissemination of their biometric information, the alleged statutory violations actually harmed or posed a material risk in harming those privacy interests.[105] The court held that a violation of this right articulated by the statute prevented people from exercising these rights, which itself is a concrete injury-in-fact.[106] The argument from Facebook that there was no actual injury because the statutory violation was merely procedural in nature was denied.[107] The Ninth Circuit found *Rosenbach* persuasive when reasoning that the purpose

---

99 *See* Marsh, *supra* note 79.

100 *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1264, 1269, 1274 (9th Cir. 2019).

101 932 F.3d 1264 (9th Cir. 2019).

102 *Id.* at 1268.

103 *Id.* at 1267.

104 Gary R. Clark, Meghan C. O'Connor & Sarah A. Erdmann, *Ninth Circuit Rejects Article III Standing Argument for BIPA Claims*, QUARLES & BRADY LLP (Sept. 6, 2019), https://www.quarles.com/publications/ninth-circuit-rejects-article-iii-standing-argument-for-bipa-claims/ [https://perma.cc/Q9K8-6TFK].

105 *Patel*, 932 F.3d at 1272–75.

106 *Id.* at 1274.

107 *Id.* at 1274–75.

of BIPA was to protect concrete rights in privacy, not just procedural rights.[108]

B. The Second Circuit's Application of the Law

The Second Circuit has found that plaintiffs have failed to allege a real injury, or a risk of one, for statutory violations of biometric privacy. In previous cases, the Second Circuit had also applied *Spokeo* by identifying a procedural right conferred by Congress and considering whether this right was at a "risk of real harm" upon a procedural violation.[109] The court used this reasoning in *Santana v. Take-Two Interactive Software, Inc.*,[110] where plaintiffs alleged BIPA violations when a video game maker enabled users to create an individualized avatar through face-scanning technology.[111] Before doing so, users had to agree to terms and conditions that stated that facial scans might be "recorded or screen captured during gameplay."[112]

The court assumed, without deciding, that BIPA was enacted to "prevent the unauthorized use, collection, or disclosure of an individual's biometric data," but it found that none of the violations were a material risk of harm to privacy interests of plaintiffs because the defendant informed users of the face scan in the terms and conditions.[113] The court held that there was no harm for the purposes of standing because the plaintiffs failed to show that the procedural violations committed would create a material risk that would actually occur.[114] *Santana* was the first appellate court to dismiss a lawsuit for lack of standing where procedural violations of BIPA were alleged, and therefore the subsequent Ninth Circuit ruling in *Patel* was in direct tension with it.[115] When the Supreme Court denied certiorari after

---

108 *See id.* at 1273.

109 Strubel v. Comenity Bank, 842 F.3d 181, 190 (2d Cir. 2016) (quoting Spokeo, Inc. v. Robins (*Spokeo I*), 578 U.S. 330, 341 (2016)).

110 717 F. App'x 12 (2d Cir. 2017).

111 *Id.* at 14.

112 *Id.* at 13–14.

113 *Id.* at 15.

114 While the defendant did not inform users on the retention period in violation of BIPA, the court found no material risk of harm because plaintiffs could not prove that the defendant would fail to properly destroy their biometric data when they were supposed to, or that they lacked proper protocols to do so. *Id.* at 16–18. Nor did the plaintiffs allege that consumer data was being disseminated or accessed by third parties without their consent, even though they claimed the defendant was transmitting and storing user biometric identifiers in a way that risked tracing the information back to the user's identity. *Id.*

115 *See* Laura Maechtlen, *The Second Circuit Weighs in on Tidal Wave of Class Actions Under the Illinois Biometric Privacy Act*, SEYFARTH SHAW LLP: WORKPLACE CLASS ACTION BLOG (Nov. 29, 2017), https://www.workplaceclassaction.com/2017/11/the-second-circuit-weighs-

Facebook appealed the *Patel* ruling, it declined to resolve the resulting circuit split.[116]

C. The Seventh Circuit's Application of the Law

The Seventh Circuit has generally landed between the decisions reached by the Ninth and Second Circuits, finding Article III standing for violation of certain sections of BIPA, but not others. In *Bryant v. Compass Group USA, Inc.*,[117] employees for a call center had to scan and use fingerprints to use the vending machine in a workplace cafeteria.[118] The plaintiffs filed a class action and alleged violations of Section 15(b) and Section 15(a) of BIPA.[119] Section 15(b) prescribes the informed consent and written policy requirement of the Act, while Section 15(a) provides the obligation private entities have to disclose a data retention schedule and guidelines for destroying collected biometric data.[120] The Seventh Circuit in *Bryant* held that a violation of Section 15(b) amounts to an injury-in-fact to satisfy Article III standing without alleging further injury.[121] Because the company failed to follow BIPA regulations by collecting employee fingerprints without giving them opportunity to consider whether the terms of the collection and usage were acceptable, employees were deprived of this right, and injury-in-fact was sufficiently established by this statutory violation.[122]

In *Bryant*, the Seventh Circuit interpreted the *Spokeo* decision as allowing the legislature to decide when there has been a concrete injury "previously inadequate in law,"[123] and that this injury did not have to be tangible.[124] On the other hand, the claim under 15(a) was not a concrete and particularized injury when the company did not make publicly available its written policy detailing a retention sched-

---

in-on-tidal-wave-of-class-actions-under-the-illinois-biometric-privacy-act/ [https://perma.cc/3FDN-6GA7]; *see* discussion *infra* Section III.A.2.

116 *See Supreme Court Leaves the Door Open for Expansive Biometric Privacy Lawsuits*, *supra* note 33.

117 958 F.3d 617 (7th Cir. 2020).

118 *Id.* at 619–20.

119 *Id.* at 617–20.

120 *Id.* at 617–25.

121 *Id.* at 626–27.

122 *Id.*

123 *Id.* at 621 (quoting Spokeo, Inc. v. Robins (*Spokeo I*), 578 U.S. 330, 341 (2016)).

124 *Id.* at 621–24. The court mainly relied on Justice Thomas's concurrence in *Spokeo* to reach its decision, where he distinguished between "private" and "public" rights. *See id.* at 623–24. Because the plaintiffs' claim in *Bryant* concerned their own personal biometric information, the court determined this to be a "private" right that was sufficient to show "injury-in-fact without further tangible consequences." *Id.* at 624.

ule and guidelines for future destruction of biometric information.[125] The court reasoned that the right conferred by 15(a) was a public right, not a private one owed to individuals.[126]

The Seventh Circuit later revisited the Section 15(a) issue and this time, reached a decision that comported more with the Ninth Circuit, which found Article III standing for violations of both Sections 15(a) and 15(b) of BIPA. In *Fox v. Dakkota Integrated Systems, LLC*,[127] the Seventh Circuit held that a violation of Section 15(a) was also a concrete injury sufficient for standing when a company failed to develop a data collection policy, which resulted in retaining a former employee's biometric data unlawfully after she left the company.[128] Later, in *Thornley v. Clearview AI, Inc.*,[129] however, the court reiterated its stance on public and private rights.[130] In *Thornley*, the defendant collected the plaintiff's biometric identifiers and sold them to third parties in violation of section 15(c) of BIPA,[131] which prohibits private entities from selling, leasing, trading, or profiting from an individual's biometric identifiers.[132] The Seventh Circuit reasoned that a violation of this section breached a duty to the overall public, not an individual plaintiff.[133] Thus, similar to the ruling in *Bryant*, the court held that there was no Article III injury for the *Thornley* plaintiffs.[134]

While the Seventh Circuit was willing to find standing in certain circumstances, it distinguished between violations of different types of rights that constituted Article III injury.[135] Still, by clarifying that it was possible for there to be Article III standing from procedural violations of both Section 15(a) and 15(b), the Seventh Circuit represented a movement toward allowing biometric privacy claims in federal court. This ruling contrasted with that of the Second Circuit, which rejected Article III standing for both sections 15(a) and (b) of BIPA.[136] Although federal courts have not had the chance to fully apply the new instructions laid down in *Ramirez*, the current circuit split highlights the uncertainty of courts on how to generally approach the standing

125 *Id.* at 626.
126 *Id.*
127 980 F.3d 1146 (7th Cir. 2020).
128 *Id.* at 1154–55.
129 984 F.3d 1241 (7th Cir. 2021).
130 *Id.* at 1245.
131 *Id.* at 1242–43.
132 740 ILL. COMP. STAT. 14/15(c) (2021).
133 *Thornley*, 984 F.3d at 1245–47.
134 *Id.* at 1248.
135 *See id.*
136 *See supra* Section II.B.

doctrine for biometric privacy litigation, which will likely continue in the future.

III. Interpreting *Spokeo*, *Ramirez*, and Private Rights of Action

The circuit split regarding standing in cases concerning biometric privacy violations creates issues for both plaintiffs and defendants. An increasing number of cases have been brought under BIPA in recent years,[137] particularly due to the 2019 Illinois Supreme Court decision in *Rosenbach*,[138] which opened the door for BIPA litigation by holding that plaintiffs do not have to demonstrate actual harm to qualify as an "aggrieved" person under the Act.[139] Afterwards, the Ninth and Seventh Circuits, finding that there was concrete injury when defendants did not comply with BIPA provisions, led to increased BIPA litigation in federal court brought by plaintiffs under diversity jurisdiction.[140] Within the influx of BIPA cases, large corporations also continue to remove cases from state court to federal court under diversity jurisdiction, and then move to dismiss for lack of Article III standing.[141] There have even been instances where the plaintiffs themselves have asked the court to remand the case from federal court back to state court by alleging lack of concrete injury-in-fact for standing.[142] It is clear that the standing doctrine is being strategically manipulated by litigants to find favorable fora—a situation that would not be necessary if the courts were more unified in approach.

Inconsistent application of the law across the country also leads to uncertainties about when and where to file suit, unpredictable outcomes, and raises a question of inherent unfairness when different jurisdictions are enforcing the same law in different manners. Although litigants have the option to choose the most advantageous forum to litigate BIPA claims, this could potentially raise litigation costs and inefficiency in reaching consistent outcomes. Federal courts should apply a uniform standard to decrease such future uncertainties and contradictory results.

---

137 *See supra* Section II.B. From 2018–2019, about 213 BIPA cases were filed in Illinois state and federal courts. Winter et al., *supra* note 98.

138 Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1201–02 (Ill. 2019).

139 Winter et al., *supra* note 98.

140 Marsh, *supra* note 79.

141 *See, e.g.*, Hazlitt v. Apple Inc., 500 F. Supp. 3d 738 (S.D. Ill. 2020), *vacated sub nom. In re* Apple Inc., No. 20-8033, 2021 WL 2451296 (7th Cir. Jan. 22, 2021).

142 *See, e.g.*, Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 620 (7th Cir. 2020).

Section A of this Part argues that courts reviewing biometric privacy cases should apply *Ramirez* in a manner that recognizes biometric privacy violations as concrete harms sufficient for Article III standing. The *Ramirez* decision illustrates that courts still have an inadequate understanding of privacy harms, and to apply the holding literally in biometric privacy suits would reach an absurd result. Therefore, the circuit split in biometric privacy cases will remain relevant even after *Ramirez*, because not only have courts been unable to fully appreciate *Ramirez* yet, they also cannot do so within the biometric privacy context without leading to these absurd results. If such results would arise from a strict application of *Ramirez*, the alternative is to look at the ways the biometric privacy legal landscape has already been shaped by the previous circuit split.

Section B reveals that, by stripping away the protections afforded by statute, corporations and businesses have little incentive to do their best in safeguarding consumers' sensitive biometric information. In addition, the *Ramirez* holding should not be interpreted literally because of a separation of powers argument. In this sense, the federal judiciary should not overstep the authority of state legislators by denying standing to rights expressly given by statutes, because it should be the prerogative of the legislative branch, not the courts, to decide substantive rights. Finally, Section C argues that based on the biometric privacy legal landscape already developed, courts should follow the Ninth Circuit's approach until the Supreme Court further clarifies standing in this context.

A. Courts Should Apply Ramirez *to Find Concrete Injury for Biometric Privacy Violations*

In *Ramirez*, the Supreme Court made it clear that for standing in federal courts, plaintiffs must show an additional injury beyond a statutory violation—harm of a protected right that has a "close historical or common-law analogue" recognized by courts in the past.[143] The Court added, however, that this "does not require an exact duplicate in American history and tradition."[144] This statement was meant to clarify the rather ambiguous direction given in *Spokeo*, which called courts to look at both the judgment of Congress and a harm that was traditionally a basis for lawsuits in English or American courts, without elaborating on how to do so.[145] The *Ramirez* decision instructs that

143 TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2204 (2021).

144 *Id.*

145 *See id.*

plaintiffs have standing to pursue violations of laws creating a legal right only if the harm has an analogue historically or at common law, though the injury does not need to be an exact match.[146] For example, in *Ramirez*, the Court likened the harm when consumers were mistakenly identified as potential terrorists to the tort of defamation.[147] Because publication of the defaming statement is a requirement for defamation, and there, the false identification had only been retained for most of the plaintiffs in the suit and not disseminated to third parties, the Court found an insufficiently close relationship to confer standing for those plaintiffs.[148] The idea was that they suffered no concrete injury because there cannot be injury to their reputation without the publication or dissemination of information.[149]

Courts reviewing biometric privacy cases should follow the Ninth Circuit's model and apply *Ramirez* in a way that recognizes biometric privacy violations as concrete harms sufficient for Article III standing. Because biometric identifiers are unique, sensitive, and different from other types of personal information,[150] courts should not follow the *Ramirez* decision the way it was applied in the *Ramirez* context, and instead return to the legal analysis that already exists under the various BIPA cases in instances regarding biometric data. Fundamentally, the facts of *Ramirez* and the resulting alleged harm are distinguishable from and do not apply to biometric privacy suits. The *Ramirez* plaintiffs claimed there had been reputational harm based on inaccurate credit files because of the defendant's failure to use reasonable procedures to ensure accuracy under FCRA as well as a failure to notify them that a problem existed with their record at all.[151] On the other hand, biometric privacy suits will mainly concern harms stemming from improper *collection* and *storage* of biometric data.[152] Under BIPA, this occurs when entities collect and store biometric identifiers without proper notice, obtainment of written consent, and disclosures like a written biometric privacy policy for consumers.[153] This type of injury to an individual is not reputational; the focus is not on adverse effects from the publication of inaccurate information, but the harvesting of the most sensitive biological data from our bodies. The ar-

146 *Id.*

147 *Id.* at 2208–09.

148 *Id.* at 2209–13.

149 *Id.*

150 *See supra* Section I.B.

151 *See Ramirez*, 141 S. Ct. at 2202.

152 *See supra* Section I.B.

153 *See supra* Section I.B.

gument against finding standing in *Ramirez* does not apply because the harm identified by biometric privacy statues is nothing like the harm of defamation. Thus, even if there is no dissemination to third parties, or "publication," courts should still recognize concrete harms in instances of biometric privacy violations.

In fact, *Ramirez* identified several privacy torts, such as intrusion upon seclusion, as harms that meet the articulated criteria for standing.[154] The intrusion upon seclusion tort, unlike defamation, does not require the dissemination of private information.[155] By specifically recognizing a privacy tort that does not require disclosure of information, *Ramirez* implies that there can be types of privacy violations that are concrete injuries sufficient for standing even without dissemination to third parties.[156] Violations of biometric privacy statutes should be considered such a harm, especially because the harm protected against is not reputational.

1. Courts Have Difficulty Understanding Privacy Harms

Courts should also not read *Ramirez* literally because courts are uncertain about how to approach privacy violations,[157] and *Ramirez* is still ambiguous enough that courts will likely continue to struggle to interpret the holding. Interpreting *Ramirez* in a way that completely shuts the door for potential litigants in federal courts is too hasty in the era of mass data collection and could lead to under deterrence and other undesirable results. Although *Ramirez* clarifies *Spokeo* in many ways, it also adds several layers of ambiguity to the already muddled doctrine. For one, how close does the injury approximately need to be to its supposed historical or common law analogue? Where is the cut-off point in the timeline for a harm to be "historical"? Given these ambiguities, courts should be wary to apply *Ramirez* at its face value to a concept that is already difficult for courts to grapple with, like modern privacy harms.

Lower courts had already reached widely different results in their attempts to apply the previous *Spokeo* decision to biometric data privacy harms. For example, both the Ninth and Seventh Circuits rightfully saw that BIPA was enacted in order to give Illinois residents the

154 *See Ramirez*, 141 S. Ct. at 2204.

155 *See* Gadelhak v. AT&T Servs., Inc., 950 F.3d 458, 462 (7th Cir. 2020) (explaining that tort of intrusion upon seclusion rests upon defendants' invasion of privacy).

156 *See Ramirez*, 141 S. Ct. at 2204.

157 *See, e.g.*, Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 15 (2d Cir. 2017); Patel v. Facebook, Inc., 932 F.3d 1264, 1270 (9th Cir. 2019).

right to control the collection, storage, and use of their biometric data, and therefore, violating the act was equivalent to violating peoples' concrete interests in that right.[158] The circuits, however, diverged when it came to section 15(a) of BIPA, which mandates companies to make publicly available its written policy on biometric data, including its retention schedule and guidelines for future destruction of the biometric information it has collected.[159] When Section 15(a) was at issue, *Bryant* found no concrete injury because it found that a failure to develop and publish a data collection policy is a bare procedural violation.[160] Yet later in *Dakkota*, the Seventh Circuit would go on to acknowledge that there could be Article III standing in Section 15(a) where no written retention and destruction policy for biometric data was provided and the defendant failed to destroy biometric data after the plaintiff left the company.[161] The Seventh Circuit distinguished *Bryant* from *Dakkota* by stating that even though failing a general and public duty to disclose data retention and destruction policies was not an adequate concrete harm, the harm alleged in *Dakkota* was one of compliance resulting in unlawful retention.[162] Namely, the defendant's noncompliance with BIPA by not developing and publicly disclosing a data collection policy led to an unlawful retention of biometric identifiers, which is a sufficient concrete injury.[163]

Then later, the Seventh Circuit in *Thornley* also found no injury from a section 15(c) violation, analogizing the section with its previous reasoning in *Bryant* for section 15(a).[164] The court found that the defendant violated a public duty rather than a private duty for its sale of the plaintiff's biometric identifiers, and so the plaintiff had no standing in federal court.[165] Plaintiffs thus have standing to pursue a claim in the Seventh Circuit when their biometric identifiers are collected and retained without proper notice and consent, but they do not have standing when a company fails to provide consumers with an adequate data collection policy or even sells their biometric identifiers to third

158 *See supra* Part II.

159 *See supra* Part II.

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

161 Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146, 1153–56 (7th Cir. 2020).

162 *Id.*

163 "She accuses Dakkota of violating the full range of its section 15(a) duties by failing to develop, publicly disclose, *and comply with* a data-retention schedule and guidelines for the permanent destruction of biometric data when the initial purpose for collection ends." *Id.* at 1154.

164 Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1245–49 (7th Cir. 2021).

165 *Id.* In *Bryant*, the Seventh Circuit similarly determined that the defendant's failure to follow the statutory publication requirements violated a duty to the public and not to the private plaintiff, and so the plaintiff had no standing in federal court. *Bryant*, 958 F.3d at 626.

parties for profit.[166] This discrepancy just within the Seventh Circuit between interpretations of different provisions of BIPA illustrates that courts perhaps have a sense that there was concrete harm to plaintiffs, but are unsure how to exactly square those harms with the existing standing doctrine.

But generally, courts tend to not have a clear understanding of privacy harms at all. For instance, the Second Circuit's *Santana* case assumed that the purpose of BIPA was "to prevent the unauthorized use, collection, or disclosure of an individual's biometric data" and found that the collection and disclosure of facial scans did not pose a material risk of harm to this interest, particularly because plaintiffs knew their data was being collected and did not allege that the data might be improperly accessed by third parties.[167] The outcomes of *Santana*, *Ramirez*, and others like them[168] result from an overly narrow interpretation of privacy harm that focuses on the dissemination of information leading to physical proof of harm, such as identity theft or tangible financial losses.[169] But what is the point of a protective privacy law if redress is only available to victims after the very situation the law is trying to protect against actually happens? Retroactive remedies do not change the fact that someone's data was already compromised and their privacy invaded as a result. This is more of a concern when it comes to biometric privacy, where biometric identifiers are uniquely sensitive to the individual and cannot be changed like a password whenever there is a data breach.[170]

2. *Courts Applying* Ramirez *Literally Will Lead to Absurd Results*

Additionally, *Ramirez* should not be read and applied literally because to do so would lead to absurd results. There have already been scholars who have pointed out that if *Ramirez*'s instructions are read literally, and only violations of rights protected historically or at common law are allowed in federal court from now on, this could

166 *Dakkota*, 980 F.3d at 1153–56 (failure to provide written policy and failure to destroy data); *Bryant*, 958 F.3d at 626 (failure to provide adequate data collection policy); *Thornley*, 984 F.3d at 1245–49 (sale of biometric identifiers).

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

168 Similarly, in *Rivera v. Google, Inc.*, 366 F. Supp. 3d 998 (N.D. Ill. 2018), the court found that there was no material harm because the plaintiffs did not dispute that their face templates had not yet been shared to third parties, or that there had been unauthorized access to their biometric information. *Rivera*, 366 F. Supp. 3d at 1006–07.

169 *See* Solove & Citron, *supra* note 53, at 741.

170 *See supra* Section I.B.

drastically limit the ability to sue under countless already established laws.[171] Many well-litigated federal laws that plaintiffs depend upon are congressionally created statutory rights with seemingly no historical or common law equivalent.[172] In his dissent in *Ramirez*, Justice Thomas used the example of copyright law, which gives copyright holders the right to sue for infringement for statutory violations without having to show monetary loss.[173] If *Ramirez* is applied literally, then there will no longer be standing for many of these existing laws; surely the Supreme Court did not intend for that kind of massive upheaval throughout various sectors when litigants across the country are suddenly cut off from their desired forum.

Furthermore, preventing people from being able to bring biometric privacy suits in federal court could impact the deterrent effect intended by BIPA and biometric statutes similar to it. There has to be an incentive for companies and businesses to meet the reasonable standard of care in collecting, using, and safeguarding peoples' biometric information. The monetary awards to plaintiffs for violations of protective measures are a way to nudge these businesses to clean up procedures and ensure that biometric identifiers are being handled with the maximum possible vigilance, as illustrated by BIPA's provisions awarding more damages if the violation was reckless or intentional.[174] Entities have less incentive to make substantive changes when there is a lesser chance of noticeable penalties.[175] Because of the higher level of responsibility that comes with handling extremely sensitive information, these entities should be appropriately scrutinized and regulated. It would make little sense to remove an extra layer of protection from the plaintiffs' arsenal by blocking another avenue of accountability in federal court.

Biometric data falls into the category of particularly sensitive information, and its release could permanently increase risk to the indi-

---

171 Erwin Chemerinsky, *What's Standing After* TransUnion LLC v. Ramirez, N.Y.U. L. REV. ONLINE 269, 283 (2021).

172 *Id.* (pointing out Freedom of Information Act, Family and Medical Leave Act, Fair Housing Act, and many others as examples of such laws that would be in danger if *Ramirez* is applied literally in the future).

173 TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2217 (2021) (Thomas, J., dissenting).

174 *See* 740 ILL. COMP. STAT. 14/20 (2021).

175 TransUnion provides the perfect example of such an entity. *Ramirez* was not the first time that TransUnion was sued for inaccurately reporting someone as a potential terrorist or drug trafficker. *See* Cortez v. Trans Union, LLC, 617 F.3d 688 (3d Cir. 2010). But in the aftermath, TransUnion still failed to implement any meaningful or preventative measures. Ramirez v. TransUnion LLC, 951 F.3d 1008, 1021 (9th Cir. 2020) (TransUnion "made surprisingly few changes" after a small penalty in *Cortez*).

vidual because it is unique to that person and cannot be readily changed.[176] There are already methods of printing a replica of someone's fingerprint, creating iris images for iris scanners, and even "fooling voice scanners with sound-morphing tools."[177] Preventing these privacy harms is the reason biometric privacy and other privacy statutes are enacted in the first place. Therefore, retroactive remedies after the fact are quite useless.[178] This goal of protecting the public's privacy interests was recognized by the Ninth Circuit in *Patel* when the court reasoned that BIPA was enacted to protect those privacy interests by giving people the right to control their biometric information; therefore, a violation of this right would amount to a concrete injury.[179]

Part of the issue are the vague standards set by *Spokeo* that left room for lower courts to determine the nature of privacy harms, leading to a constrained interpretation as courts search for the basis of traditional harms found in common law.[180] Although *Ramirez* offered some clarification on the matter, its holding—like *Spokeo*—was particular to the FCRA and to the reasoning that most of the plaintiffs' erroneous information had not yet been sent to third parties.[181] But the lower courts should not apply these holdings too broadly for cases of privacy harm, especially those concerning biometric information, because of the unique and unalterable nature of biometric identifiers. Cases involving sensitive biometric data should be distinguished because at the instance dissemination occurs, the data is forever compromised and cannot be changed or fixed like inaccurate credit reports.[182] Being reported as a potential terrorist is less than ideal, but there is something much more intimate regarding data that is part of some-

176 *See* Chaminda Hewage, *Stolen Fingerprints Could Spell the End of Biometric Security – Here's How to Save It*, CONVERSATION (Aug. 20, 2019, 8:06 AM), https://theconversation.com/stolen-fingerprints-could-spell-the-end-of-biometric-security-heres-how-to-save-it-122001 [https://perma.cc/MG6R-RKKE].

177 *Id.*

178 *See* Daniel Solove, *The Trouble with* Spokeo*: Standing, Privacy Harms, and Biometric Information*, TEACHPRIVACY (Jan. 6, 2019), https://teachprivacy.com/trouble-with-spokeo-standing-privacy-harms-and-biometric-information/ [https://perma.cc/FU87-EKG6] (pointing out that many privacy laws articulate a right to deletion of data, erasure, or a right to be forgotten, such as the Children's Online Privacy Protection Act, the EU General Data Protection Regulation, and the CCPA).

179 *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1270–75 (9th Cir. 2019).

180 *See* Matthew S. DeLuca, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439, 2463 (2018).

181 *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2211–13 (2021).

182 Hewage, *supra* note 176.

one's body—the difference between losing agency over your name temporarily or your fingertips permanently.

In situations involving biometric data, courts using the standing doctrine to deny privacy suits leave the public without much protection during the modern age of mass data collection. In the absence of a comprehensive national data security law, personal data is currently regulated by a myriad of federal and state laws including HIPPA, the Gramm-Leach-Bliley Act, and state laws like the CCPA.[183] However, due to limited enforcement mechanisms, as well as retroactive remedies, the public is still left vulnerable to the exposure of their data.[184] Leaving the ability to sue under longstanding statutes with statutorily created rights of action in doubt and stripping away protective measures in the handling of unique biometric identifiers are the undesirable and absurd outcomes that would result from applying *Ramirez* literally.

B. The Supreme Court in Ramirez *Has Encroached on the Legislative Branch*

Courts should also read *Ramirez* narrowly in its application because to do otherwise would undoubtedly undermine separation of powers. The Supreme Court in *Ramirez* has encroached on the legislative branch by denying the legislative ability to create statutory rights and stating that Congress cannot "transform something that is not remotely harmful into something that is."[185] Even though the *Ramirez* Court stated that separation of powers was actually being facilitated by restricting standing,[186] limiting the congressional power to provide rights of actions appears to have exactly the opposite effect. This is especially so because Congress has historically been able to create rights sufficient for Article III standing without judicial limitations.[187] The legislative branch is in the best position to address new concerns because it is capable of an agile and complete policy response, and to place limitations on this ability now would arguably result in the stagnation of progress.[188]

---

183 *See supra* notes 12–20, 65–77 and accompanying text.

184 *See* Daniel J. Marcus, *The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information*, 68 DUKE L.J. 555 (2018).

185 *Ramirez*, 141 S. Ct. at 2205 (quoting Hagy v. Demers & Adams, 882 F.3d 616, 622 (6th Cir. 2018)).

186 *Id.* at 2203.

187 *Id.* at 2220–21 (Thomas, J., dissenting).

188 Chemerinsky, *supra* note 171, at 287 (pointing out that many serious harms are recog-

Similarly, inherent within the various biometric privacy legislation enacted, including BIPA, are rights regarding peoples' biometric privacy, including the right to have control over biometric information. The Ninth Circuit interpreted BIPA to incorporate a right to understand the collection and use of biometric identifiers in order for people to be a part of the decision-making process of their own personal data.[189] The CCPA, which includes biometric data in its regulations,[190] also has a right of notice provision where consumers must be informed about the biometric data that is being collected, used, or stored by a company.[191] Part of the right of notice is the mandate that people should know how long an entity will hold onto the biometric data until it is permanently destroyed.[192] It can be interpreted that by enacting laws like the CCPA or BIPA, various legislatures have determined that various types of privacy harms exist beyond just the dissemination of data, for which there should be sufficient statutory remedies or redress available.

Federal court decisions regarding the standing doctrine for biometric privacy issues will influence how effectively state legislatures can protect biometric data.[193] BIPA in particular allows for a private right of action that emphasizes that the legislature intended for those individuals who have been injured in this manner to pursue relief in court.[194] It is significant that BIPA, out of all the other state biometric privacy statutes, has a private right of action, especially because most other biometric privacy statutes do not.[195] The wording of a statute is a sign of how the legislature views the severity of the harm and can help courts determine if a violation of that statute sufficiently leads to concrete injury. For BIPA, the Illinois legislature decided that biometric

---

nized today, such as "[d]iscrimination based on race, sex, religion, or sexual orientation" that would not have been recognized in the past or at common law).

189 *See* Patel v. Facebook, Inc., 932 F.3d 1264, 1269–75 (9th Cir. 2019).

190 CAL. CIV. CODE § 1798.140(b) (West 2020).

191 *Id.* §§ 1798.100, 1798.110, 1798.115.

192 *Id.*

193 *See* Michelle Jackson, *Opting Out: Biometric Information Privacy and Standing*, 18 DUKE L. & TECH. REV. 293, 304 (2020).

194 *See* Solove, *supra* note 178 (arguing that legislatures do not "give out private rights of action loosely" and that "judges ought to show a lot more respect for the legislature's determination").

195 As of early 2021, BIPA is the only state biometric privacy law that provides for a private right of action, although a proposed New York biometric privacy law mirrors BIPA and includes a similar private right of action. Glenn T. Graham & Paul A. Rosenthal, *Proposed NY Biometric Privacy Act Would Allow Private Right of Action*, KELLEY DRYE & WARREN LLP (Jan. 8, 2021), https://www.adlawaccess.com/2021/01/articles/proposed-ny-biometric-privacy-act-would-allow-private-right-of-action/ [https://perma.cc/CDE3-QRJG].

privacy was important enough to allow a remedy within the law and that a private right of action is a proper enforcement tool.[196] As discussed previously, the legislative branch often creates small damages to increase incentives for entities to improve their procedures.[197]

It is not up to the courts to use the standing doctrine to supplant injuries identified by statutes with its own judgment.[198] In his scathing dissent in *Ramirez*, Justice Thomas pointed out that the majority decided on its own that the Constitution "prohibits consumers from vindicating their rights in federal court," and this was "despite Congress' judgment that such misdeeds deserve redress."[199] Justice Kagan also dissented, pointing out that the Court transformed standing law "from a doctrine of judicial modesty into a tool of judicial aggrandizement."[200] While the fear of a flood of litigation is valid—and arguably already in the midst of occurring[201]—the standing doctrine should not be a tool used by courts to usurp the will of legislatures.[202] Denying standing because the injury is not "real" enough to meet the standard interpreted by courts is also to decide the "substantive content of those rights"[203] and allows courts to second guess what the legislative branch judged as actionable under the law. This can prevent effective legislative action moving to address arising instances of harm before such harms can be completed.[204] The state legislature in Illinois has determined private rights of action should exist for biometric privacy violations because they are so distinct from other types of harms. If the legislative branch has identified a new type of harm, then according to the separation of powers, the judicial branch should not restrict this ability by becoming the gatekeeper of what it subjectively believes is a real injury or not. Thus, lower courts should also not read the *Ramirez* decision as instructions or permission to encroach upon the separation of powers.

---

196 *See* Solove, *supra* note 178.

197 *See supra* Section III.A.

198 *See* Daniel Townsend, *Who Should Define Injuries for Article III Standing?*, 68 STAN. L. REV. ONLINE 76, 84 (2015) ("Deciding which injuries are worth vindicating more properly belongs in the policy realm than the judicial one.").

199 TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2214 (2021) (Thomas, J., dissenting) ("The Constitution does no such thing.").

200 *Id.* at 2225 (Kagan, J., dissenting).

201 *See* Marsh, *supra* note 79.

202 Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 458 (2017).

203 *Id.*

204 *Id.* at 459 (criticizing how "scrutiny of harms [by federal courts] undermines the legislature's ability to act to prevent harms proactively, rather than only addressing completed harms").

Conclusion

In the wake of *Spokeo*, a circuit split developed as courts continued to grapple with the standing doctrine. Now after *Ramirez*, courts should apply the holding narrowly to instances of biometric privacy violations in order to avoid the absurd result of closing the door to federal court, taking away protective measures, and usurping the will of the legislative branch by undermining the separation of powers. Privacy issues are becoming increasingly prevalent and legislated, and it is crucial for courts to reach a common consensus to avoid widely inconsistent application of the law and to set clear standards for businesses and private entities collecting and utilizing biometric data. The distinctiveness of biometric data, as well as the accelerating spread of its use, should concern courts as much as it has concerned the legislatures that have articulated protections in the form of statutes such as BIPA. For this reason, courts should avoid dismantling the protections granted and allow standing in instances of people asserting their biometric privacy rights.