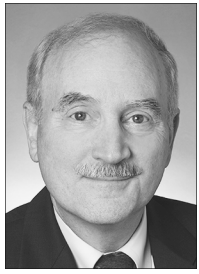
THE NEXT BIG THING: CURRENT ISSUES UNDER THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT*

John L. Ropiequet, April Falcon Doss, and Valerie G. Pennacchio



John L. Ropiequet

April Falcon Doss

Valerie G. Pennacchio

John L. Ropiequet is Of Counsel to the Litigation Group at Saul Ewing Arnstein & Lehr, LLP's Chicago office. He is a graduate of The Johns Hopkins University and Northwestern Pritzker School of Law. John is immediate past Chairman of the Conference on Consumer Finance Law, a Fellow of the American College of Consumer Finance Lawyers, and co-editor of the Annual Survey on Consumer Finance Law *in* The Business Lawyer. *He is also co-editor of the 2018 supplement to* The Law of Truth in Lending *and a frequent contributor to the* Consumer Finance Law Quarterly Report *and other publications.*

April Falcon Doss is a partner at Saul Ewing Arnstein & Lehr LLP's Baltimore office, where she chairs its Cybersecurity and Privacy Practice Group. She is a graduate of Yale University, Goucher College, and the University of California, Berkeley, Boalt Hall School of Law.

Valerie G. Pennacchio is a former Associate at Saul Ewing Arnstein & Lehr LLP's Newark, New Jersey office. She is a graduate of Cornell University and Seton Hall University School of Law.

I. INTRODUCTION

Although the Illinois Biometric Information Privacy Act (BIPA)[1] was enacted in 2008, its provisions have only recently begun to attract widespread attention among businesses that may have run afoul of its require-

---

* This article is adapted from an earlier version published in the *Banking and Financial Services Policy Report.* Reprinted with permission.

1. Biometric Information Privacy Act, 2007 Ill. Laws 994 (codified in scattered sections of 740 ILL. COMP. STAT. 14) (2008).

ments. The Act protects individuals' unique biometric identifiers, like fingerprints and facial geometry, by requiring persons to make disclosures and obtain written releases prior to collecting biometric data. Starting in 2015, after a variety of decisions were issued on motions at the trial court level, two decisions in 2019—one from the Illinois Supreme Court[2] and one from the U.S. Court of Appeals for the Ninth Circuit[3]—have made it clear that failure to comply with the BIPA's requirements can subject companies to substantial class action liability wherever Illinois residents may be involved.

As a result, potentially massive class actions are flooding the federal courts as well as Illinois state courts. The cases deal with a wide variety of ways in which biometric data allegedly has been collected by major technology companies and other businesses without complying with the requirements of BIPA. Among the more recent filings are complaints about: a company that stores the biometric data of other companies' employees;[4] a casino that uses facial geometry scans to identify thousands of customers a day;[5] a computer application on users' devices that uses such technology;[6] a store surveillance system that employs facial recognition technology;[7] uploading online customers' voice recordings;[8] application of facial recognition technology to online customers' uploaded photographs;[9] using employees' fingerprint data as digital timecards;[10] and using pharmacists' fingerprint data to access the store's computer system.[11]

2. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, 129 N.E.3d 1197 (Ill. 2019). The complaint was filed in the Circuit Court of Lake County, Illinois in January 2016. Complaint, Rosenbach v. Six Flags Entm't Corp., No. 16 CH 13 (Lake Cty. Cir. Ct. Jan 7, 2016).

3. Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019), *cert. denied*, No. 19-706, 2020 WL 283288 (U.S. Jan. 21, 2020) (mem.). The complaint was filed in the Northern District of California in August 2015. Amended Complaint, *In re* Facebook Biometric Info. Privacy Litig., No. 3:15-cv-03747-JD (N.D. Cal. Aug. 28, 2015).

4. Class Action Complaint and Jury Demand, Ragsdale v. Amazon Web Servs., Inc., No. 2019CH13251 (Cook Cty. Cir. Ct. Nov. 15, 2019).

5. Complaint, Adams v. Des Plaines Dev. L.P., No. 19L893 (Will Cty. Cir. Ct. Oct. 18, 2019).

6. Class Action Complaint, Acaley v. Vimeo, Inc., No. 2019CH10873 (Cook Cty. Cir. Ct. Sept. 20, 2019).

7. Complaint—Class Action and Demand for Jury Trial, Brunson v. Home Depot, Inc., No. 1:19-cv-03970-CC (N.D. Ga. Sept. 4, 2019), ECF no. 1.

8. Class Action Complaint for Damages and Injunctive Relief, and Demand for Jury Trial, Morales v. Google.com, Inc., No. 2019CH08309 (Cook Cty. Cir. Ct. July 15, 2019).

9. Class Action Complaint, Miracle-Pond v. Shutterfly, Inc., No. 2019CH07050 (Cook Cty. Cir. Ct. June 11, 2019), *removed*, Defendant Shutterfly Inc.'s Notice of Removal, Civil Action No. 1:19-cv-4722 (N.D. Ill. July 12, 2019), ECF no. 1.

10. Class Action Complaint, Rogers v. CSX Intermodal Terminals, Inc., No.

The Illinois Supreme Court has settled the question of whether a person is "aggrieved" within the meaning of BIPA if there is only a procedural violation of the statute but no further showing of an actual concrete harm arising from the violation. Based on that ruling, the Ninth Circuit has resolved the question of standing to sue under Article III where no further identifiable harm is shown to exist. Subsequently, the Seventh Circuit has held that BIPA claims satisfy the U.S. Supreme Court's Article III standing requirements set for in *Spokeo, Inc. v. Robins*.[12] This article will explore what the courts have done with those questions prior to the issuance of those rulings as well as the rulings themselves, and will discuss what may lie ahead in BIPA litigation. It will also consider what may happen under other statutes that protect individuals' biometric data.

II. Basic Provisions of BIPA

The statute states the following reasons for the enactment of BIPA: "Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias."[13] The statute further states the reasoning for the burdensome requirements that BIPA imposes on persons who collect biometric data belonging to Illinois residents that:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically 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.[14]

BIPA protects biometric data, defined as "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[15] Excluded from the definition are, among other things, "writing samples, written signatures, photographs, human biological samples used for scientific testing or screening, demographic data, tattoo descriptions . . . physical descriptors such as height, weight, hair color, or eye color,"[16] donated tissue, medical imaging used to diagnose or treat an illness, or genetic information regulated under the Illinois's Genetic Information Privacy Act[17] or federal Health Insurance

2019CH04168 (Cook Cty. Cir. Ct.), *removed*, Notice of Removal, Case No. 1:19-cv-02937 (N.D. Ill. May 1, 2019), ECF no. 1.

11. Class Action Complaint, Bruhn v. New Albertson's, Inc., No. 2018CH01737 (Cook Cty. Cir. Ct. Feb. 13, 2018).
12. Spokeo, Inc. v. Robins (*Spokeo I*), 136 S. Ct. 1540 (2016).
13. 740 Ill. Comp. Stat. 14/5(b) (West 2010).
14. *Id.* 14/5(c).
15. *Id.* 14/10.
16. *Id.*
17. Genetic Information Privacy Act, 1998 Ill. Laws 1046 (codified in scattered sections of 410 Ill. Comp. Stat. 513) (1998).

Portability and Accountability Act of 1996.[18] BIPA also protects biometric information, defined 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."[19]

BIPA applies only to private entities, which includes "any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency."[20] The Act does not apply to any Illinois court, or clerk, judge, or justice of the court.[21] The Act does not expressly state any territorial limitations on its coverage, so it should be construed as covering any person that collects the biometric information of any Illinois residents, regardless of where that person resides or is officed, or where the information is collected in order to accomplish the Act's protective purposes.

BIPA requires private entities to:

> Develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.[22]

Moreover, BIPA requires private entities to notify the individuals providing biometric information that such information is being stored, the purpose for collecting, storing, and using the subject's biometric data, and the length of time the data will be retained.[23] Private entities must also obtain a written release to collect biometric data.[24] Private entities are prohibited from profiting in any way from the biometric information they have collected.[25] Additionally, BIPA bars private entities from releasing biometric information unless the subject consents; the release is required by law or requested via a warrant or subpoena issued by a court; or completes a financial transaction authorized by the individual.[26]

Under BIPA, a private entity in possession of a biometric identifier or biometric information is required to protect this data "using the reasonable

18. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996); *see* 740 Ill. Comp. Stat. 14/10 (referencing Health Insurance Portability and Accountability Act of 1996 to contextualize materials excluded from definition of "biometric identifier").
19. 740 Ill. Comp. Stat. 14/10.
20. *Id.*
21. *Id.*
22. *Id.* 14/15(a).
23. *Id.* 14/15(b).
24. *Id.* 14/15(b)(3).
25. *Id.* 14/15(c).
26. *Id.* 14/15(d).

standard of care within the private entity's industry" and "in a manner that is the same as or more protective than the manner in which the private entity stores other confidential information."[27]

BIPA provides for a private cause of action and allows private individuals who are "aggrieved" by a violation of the Act to file a lawsuit for damages stemming from a violation.[28] The law provides for damages of $1,000 for each negligent violation and $5,000 for each intentional or reckless violation, with no cap on liability for class actions.[29]

III. BIPA Case Decisions in the Lower Courts

A. Federal District Court Decisions.

As might be expected for a novel claim like an alleged BIPA violation, with its apparent strict liability and potentially open-ended class action damages, the decisions that were rendered on motions to dismiss in federal district courts went in a variety of directions before the Illinois Supreme Court and Ninth Circuit rulings were made in 2019. The plaintiff's status as an "aggrieved" person within the meaning of section 20 of the Act was challenged in several cases. The plaintiff's standing to sue in the absence of a claim for actual damages was also challenged in several cases. Defendants argued that making facial scans from photographs, rather than directly from the plaintiff's face in person, qualified for the definitional exclusion in section 10 of the Act for photographs. Defendants also asserted Dormant Commerce Clause challenges based on lack of connection to Illinois.

Most of the motions stemmed from the U.S. Supreme Court's decision in *Spokeo, Inc. v. Robins*[30] in 2016, where it found that in actions under federal statutes, a bare statutory violation is not, by itself, enough to provide a plaintiff with standing to sue under Article III of the Constitution.[31] Instead, drawing from a substantial body of federal jurisprudence, the *Spokeo* Court held that in order to meet the minimum standard for standing to sue, an injured plaintiff must show that the injury is both "'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical,'" none of which can be shown by a "bare procedural violation" of a statute without more.[32]

Typical of subsequent cases that applied *Spokeo* was the Second Circuit's decision in *Strubel v. Comenity Bank*[33] a few months later. The court dealt

27. *Id*. 14/15(e).
28. *Id*. 14/20.
29. *Id*.
30. *Spokeo I*, 136 S. Ct. 1540 (2016).
31. *Id*. at 1550.
32. *Id*. at 1548–50 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).
33. Strubel v. Comenity Bank, 842 F.3d 181 (2d Cir. 2016); *See* John L. Ropiequet, *Second Circuit Applies* Spokeo *Article III Standing Analysis to TILA Claims*, 71 Consumer Fin. L.Q. Rep. 303, 304 (2017), *reprinted in* The Law of Truth in

with a putative class action under the Truth in Lending Act (TILA) for purely statutory damages allegedly arising from failing to make various billing rights disclosures as required by the TILA when the defendant bank opened credit card accounts. Although the *Strubel* court rejected a blanket claim by the bank that alleging "a bare procedural violation" of the TILA without showing any "ensuing adverse consequences" necessarily doomed the plaintiff's case across the board, it held that the plaintiff must nevertheless allege some concrete injury that flowed from each of the alleged disclosure violations.[34] The *Strubel* court engaged in a detailed analysis that found that some claims involved disclosures that protected "a core object of the TILA,"—that is, "avoid[ing] the uninformed use of credit,"—so that they could be pursued despite being intangible harms.[35] Other claims failed to show any such risk of concrete injury, so that their dismissal was upheld.[36]

The first reported BIPA decision was in *Norberg v. Shutterfly, Inc*.[37] The defendants' websites offered online photo-sharing of digital images and making hard copies and gifts from the images. The websites had a facial recognition capability used "to identify and categorize photos based on the people in the photos."[38] In a case of first impression, the court found that under "the plain language of the statute," allegations that the defendants' use of a facial recognition process without issuing a "written biometrics policy" or obtaining consent to use the plaintiff's photographs plausibly stated a BIPA claim.[39]

The next two decisions engaged in analysis of the question of whether the plaintiff qualified as an "aggrieved" person under section 20 of the Act. In *McCollough v. Smarte Carte, Inc.*,[40] the defendant used customer fingerprints as the key for storage lockers at a train station without obtaining consent from the customer or disclosing how long the data would be retained. Relying on *Spokeo*, the defendant asserted that although a technical BIPA violation was alleged, there was no allegation of harm sufficient to provide standing to sue and support subject matter jurisdiction.[41] The court found that there was no way mere retention of fingerprint data could give rise to harm that amounted to a concrete injury.[42] Accordingly, there was

---

Lending ¶ 12.02[2][d] (Lynnette S. Hotchkiss & John L. Ropiequet eds.) (Supp. 2018).

34. *Strubel*, 842 F.3d at 189.
35. *Id*. at 190 (quoting 15 U.S.C. § 1601(a)).
36. *Id*. at 191–93.
37. Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103 (N.D. Ill. 2015).
38. *Id*. at 1106.
39. *Id*.
40. McCollough v. Smarte Carte, Inc., No. 16 cv 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016), *overruled,* Bryant v. Compass Group USA, Inc., No. 20-1443, 2020 WL 2121463 (7th Cir. May 5, 2020).
41. *Id*. at *2.
42. *Id*. at *4.

no injury to establish that the plaintiff was "aggrieved," a term that is not defined in BIPA, within the meaning of the Act.[43] Taking note of a state trial court's then-recent finding in *Rosenbach v. Six Flags Entertainment Corp.* that such a plaintiff has standing to sue under BIPA, the *McCollough* court ruled that even if there might be standing in state court, that is not enough to confer federal constitutional standing, so it dismissed the case without prejudice to refiling in state court.[44]

In *Vigil v. Take–Two Interactive Software, Inc.*,[45] the defendant's MyPlayer feature scanned video game players' faces to create a personal avatar with the gamer's facial features. It obtained consent for making the scan, but allegedly gave inadequate disclosures concerning its indefinite storage of the images, it had no retention schedule, the consent was not in writing, and the information was disseminated in unencrypted transmissions without consent.[46] The New York federal district court held that although there were several alleged procedural BIPA violations,

> None of the plaintiffs' allegations of procedural violations, on their own, demonstrate a material risk of harm to the BIPA's concrete data protection interest because there is no plausible allegation that there is a material risk that the plaintiffs' biometrics may be used in a way not contemplated by the underlying use of the MyPlayer feature,

as required to provide standing to sue under *Spokeo*, *Strubel*, and *McCollough*.[47] It rejected the argument that in the *Facebook* litigation, a California district court had accepted the argument that "BIPA manifests Illinois' substantial policy of protecting its citizens' right to privacy in their personal biometric data," so that nothing more need be alleged than a violation of the statute.[48]

The *Vigil* court found that at most, "the plaintiffs' allegations are that Take–Two's storage and dissemination practices have subjected their facial scans to an 'enhanced risk of harm' of somehow falling into the 'wrong hands,' which is too abstract and speculative to support standing."[49] After discussing the plaintiffs' many arguments that there was some injury sufficient to support standing, the court agreed with the *McCollough* court's conclusion that the term "aggrieved" in BIPA requires an injury in addition to a technical violation of the statute.[50] On appeal, the Second Circuit agreed in a summary ruling that the plaintiffs failed to allege "a material risk that

43. *Id.*
44. *Id.* at *5.
45. Vigil v. Take–Two Interactive Software, Inc., 235 F. Supp. 3d 499 (S.D.N.Y.), *aff'd in part and vacated in part sub nom.* Santana v. Take–Two Interactive Software, Inc., 717 F. App'x 12 (2d Cir. 2017).
46. *Id.* at 506–07.
47. *Id.* at 511.
48. *Id.* at 510 (quoting *In re* Facebook Biometric Info. Privacy Litig., 185 F. Supp. 3d 1155, 1169 (N.D. Cal. 2016)).
49. *Id.* at 512.
50. *Id.* at 519.

their biometric data will be misused or disclosed"[51] and it was unpersuaded by "plaintiffs' attempt to manufacture an injury,"[52] but it ordered the trial court to dismiss the case without prejudice, presumably in a state court with a lesser standard for standing to sue.[53]

The search for a concrete injury resulted in dismissals of other cases. In *Barnes v. ARYZTA, LLC*,[54] for example, the lack of an alleged concrete injury led the court to remand the plaintiff employee's removed BIPA claims arising from the defendant's timekeeping procedures.[55] The result was the same in *Howe v. Speedway LLC*,[56] where the plaintiff employee's fingerprints were used for timekeeping with his unwritten consent but without the required disclosures being made. His "informational injury" was a mere procedural violation of BIPA that was insufficient to support federal jurisdictional requirements.[57]

In yet another fingerprint timekeeping case, *Goings v. UGN, Inc.*,[58] the court drew a distinction between cases like *Howe*, *Vigil*, and *McCollough*, where there was no concrete injury from mere failure to comply with the BIPA's notice and consent requirements,[59] and other cases where something more was involved. Among these were *Monroy v. Shutterfly, Inc.*,[60] where images were collected without the plaintiff's knowledge or consent; *Dixon v. Washington & Jane Smith Community–Beverly*,[61] where the defendant employer disseminated the plaintiff's fingerprint data without her knowledge or consent; and *Patel v. Facebook, Inc.*,[62] where the plaintiff's data were allegedly collected and stored without his consent.[63] The *Goings* court therefore found that "because BIPA is not essentially concerned with information disclosure, I agree with the courts in *Howe* and *Vigil* that plaintiff's alleged violation of BIPA's notice provisions is insufficient, on its own, to support federal jurisdiction."[64]

51. *Santana*, 717 F. App'x at 16.
52. *Id.* at 17.
53. *Id.* at 18.
54. Barnes v. ARYZTA, LLC, 288 F. Supp. 3d 834 (N.D. Ill. 2017).
55. *Id.* at 839.
56. Howe v. Speedway LLC, No. 17-cv-07303, 2018 WL 2445541 (N.D. Ill. May 31, 2018), *overruled,* Bryant v. Compass Group USA, Inc., 958 F.3d 617 (7th Cir. 2020).
57. *Id.* at *2, *7.
58. Goings v. UGN, Inc., No. l7-cv-9340, 2018 WL 2966970 (N.D. Ill. June 13, 2018), *overruled,* Bryant v. Compass Group USA, Inc., 958 F.3d 617 (7th Cir. 2020).
59. *Id.* at *3–4.
60. Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017).
61. Dixon v. Washington & Jane Smith Community–Beverly, No. 17 C 8093, 2018 WL 2445292 (N.D. Ill. May 31, 2018).
62. Patel v. Facebook, Inc., 290 F. Supp. 3d 948 (N.D. Cal. 2018).
63. *Id.* at 1268; *Goings*, 2018 WL 2966970, at *3–4.
64. *Goings*, 2018 WL 2966970, at *4; *see also* McGinnis v. U.S. Cold Storage, Inc.,

The California district court in *Patel* did more than find that the plaintiff had not consented to collecting and storing his facial images, however. It noted that the Supreme Court's decision in *Spokeo* "sharpened the focus on when an intangible harm such as the violation of a statutory right is sufficiently concrete to rise to the level of an injury in fact," and that Congress could create statutory rights that had never existed before.[65] Likewise, it found that "state legislatures are equally well-positioned to determine when an intangible harm is a concrete injury."[66]

The *Patel* court examined the "plain language of BIPA" to analyze the standing issue.[67] Based on that, it found that any failure to comply with BIPA's requirements constituted a concrete injury capable of sustaining federal jurisdiction:

> These provisions, along with the plain text of BIPA as a whole, leave little question that the Illinois legislature codified a right of privacy in personal biometric information. There is equally little doubt about the legislature's judgment that a violation of BIPA's procedures would cause actual and concrete harm. BIPA vested in Illinois residents the right to control their biometric information by requiring notice before collection and giving residents the power to say no by withholding consent. As the Illinois legislature found, these procedural protections are particularly crucial in our digital world because technology now permits the wholesale collection and storage of an individual's unique biometric identifiers—identifiers that cannot be changed if compromised or misused. When an online service simply disregards the Illinois procedures, as Facebook is alleged to have done, the right of the individual to maintain her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.
>
> Consequently, the abrogation of the procedural rights mandated by BIPA necessarily amounts to a concrete injury. This injury is worlds away from the trivial harm of a mishandled zip code or credit card receipt. A violation of the BIPA notice and consent procedures infringes the very privacy rights the Illinois legislature sought to protect by enacting BIPA. That is quintessentially an intangible harm that constitutes a concrete injury in fact.[68]

These "considered judgments" of the Illinois legislature were also "well-grounded in a long tradition of claims actionable in privacy law." Under the law of privacy torts, "[i]ntrusion on privacy alone can be a concrete

382 F. Supp. 3d 813, 819–20 (N.D. Ill. 2019), *overruled*, Bryant v. Compass Group USA, Inc., 958 F.3d 617 (7th Cir. 2020) (discussing how plaintiff-employee's consent for employer to collect and retain fingerprint data in violation of BIPA's notice and consent requirements but without risk of disclosure to third parties produced no concrete injury to support Article III standing).

65. *Patel*, 290 F. Supp. 3d at 952 (citing *Spokeo I*, 136 S. Ct. 1540, 1547 (2016)).

66. *Id*.

67. *Id*. at 953.

68. *Id*. at 953–54 (citing Robins v. Spokeo, Inc. (*Spokeo II*), 867 F.3d 1108, 1113 (9th Cir. 2017).

injury."[69] The court distinguished *McCollough* and *Vigil* on the ground that the plaintiffs in those cases "indisputably knew that their biometric data would be collected before they accepted the services offered by the businesses involved."[70]

The *Patel* defendants raised two other issues to avoid BIPA liability that have been given fairly short shrift by the courts in subsequent cases. In *Rivera v. Google, Inc.*,[71] the plaintiffs alleged that a BIPA violation occurred because the photographs they took on their Google Droid device were automatically uploaded to a cloud service and Google then created templates from their facial features without complying with BIPA's disclosure and consent requirements.[72] The defendant moved to dismiss on the ground that the two plaintiffs had taken their own pictures on the device; that BIPA excludes photographs as biometric information in section 10 of the Act; and that only in-person scans were included in the section 10 definition.[73] The *Rivera* court held that biometric identifiers can be collected by various means and that BIPA has no in-person requirement, so that argument failed.[74] The *Monroy* and *Facebook* courts agreed with this result.[75]

Google also argued that giving BIPA extraterritorial effect against it would violate the Dormant Commerce Clause because it would regulate commerce outside of Illinois's boundaries.[76] The *Rivera* court observed that BIPA "was not intended to and does not have extraterritorial application," and in any event, it was premature to reach any conclusions on this issue before discovery was taken.[77] The *Facebook* court reached the same conclusion when Facebook raised this argument, finding that "Facebook's facial recognition program cannot be understood to have occurred wholly outside Illinois."[78] Likewise, the *Monroy* court found that the argument was "overwrought" since the case dealt with "photographs uploaded to Shutterfly in Illinois."[79]

69. *Id.* at 954.
70. *Id.* at 955.
71. Rivera v. Google, Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017).
72. *Id.* at 1090–91.
73. *Id.* at 1092.
74. *Id.* at 1095–96.
75. Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 WL 4099846, at *3–5 (N.D. Cal. Sept. 15, 2017); *In re* Facebook Biometric Info. Privacy Litig., Case No. 3:15-cv-03747-JD, 2018 WL 2197546, at *4 (N.D. Cal. May 14, 2018) (decision on summary judgment); *In re* Facebook Biometric Info. Privacy Litig., 326 F.R.D. 535, 547 (N.D. Cal. 2018) (decision on class certification).
76. *Rivera*, 238 F. Supp. 3d at 1103 (citing Healy v. Beer Inst., Inc., 491 U.S. 324, 336 (1989)).
77. *Id.* at 1104.
78. *In re Facebook*, 2018 WL 2197546, at *4 (citing *Healy*, 491 U.S. at 332).
79. *Monroy*, 2017 WL 4099846, at *7.

B. Decisions in the Illinois Appellate Court.

Two cases have reached the appellate level in the Illinois courts. The first case, *Rosenbach v. Six Flags Entertainment Corp.*,[80] arose from the defendants' practice of requiring customers for repeat-entry passes for their amusement park in Gurnee, Illinois to have their fingerprints scanned for security purposes and to expedite reentry.[81] The named plaintiff for this purported class action was the mother of a fourteen year old boy whose thumbprint was taken without being given any information that BIPA requires of those who collect and store individuals' biometric information.[82] In addition, the defendants did not request permission to take the thumbprint, which the Act also requires.[83] The mother's complaint on behalf of her son and the plaintiff class sought statutory damages under the Act; injunctive relief to compel the defendants to give the disclosures required by BIPA and not to violate the Act in the future; and damages for common law unjust enrichment.[84]

On the defendants' motion to dismiss for lack of standing to sue and other grounds, the trial court denied the motion as to the statutory and injunctive relief counts, but granted it with prejudice on the unjust enrichment count.[85] In the interlocutory appeal of the decision, the Illinois Appellate Court held that the plaintiff was not a person "aggrieved" within the meaning of BIPA since she alleged no injury or adverse effect on her beyond the mere "technical violation" of the Act and she therefore lacked standing to sue under the Act for either statutory damages or injunctive relief.[86]

The second case, *Sekura v. Krishna Schaumburg Tan, Inc.*,[87] reached the opposite conclusion. The plaintiff there had her fingerprints scanned to enroll her as a member of the defendant tanning salon's national network.[88] Her fingerprints were scanned at each visit and her biometric information was disclosed to the salon's third-party vendor. None of the disclosures required by BIPA were given to her.[89] Although the trial court originally found that the plaintiff qualified as an "aggrieved" person within the meaning of the statute, it later reconsidered that finding in light of the appellate decision in *Rosenbach* and dismissed her case.[90]

80. Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, 129 N.E.3d 1197 (Ill. 2019).
81. *Id.* at ¶ 4.
82. *Id.* at ¶ 10 n.1.
83. *Id.* at ¶ 8.
84. *Id.* at ¶ 11.
85. *Id.* at ¶ 12.
86. Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, ¶ 28, 2017 WL 6523910, at *5 (Ill. App. Ct. Dec. 21, 2017).
87. Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175, 115 N.E.3d 1080 (Ill. App. Ct. 2018), *app. denied*, 119 N.E.3d 1034 (Ill. 2019).
88. *Id.* at ¶¶ 7–8.
89. *Id.* at ¶ 9.
90. *Id.* at ¶ 15.

At issue in the appellate court was "whether a harm or injury, in addition to the violation of the Act itself, is required in order to have standing to sue under the Act."[91] The *Sekura* court then engaged in an examination of what the BIPA required to state a cause of action, focusing on the meaning of the term "aggrieved" in section 20.[92] It observed that the Act's private right of action only required being aggrieved, not being aggrieved by the violation and by "some additional harm or injury," and that the Act provided for both statutory or actual damages, "thereby establishing that actual damages are not required to obtain relief under the Act."[93] Dictionary definitions also supported this interpretation,[94] as did BIPA's stated legislative purpose and history.[95] The court also found that the language of BIPA's private right of action was "virtually identical" to the language of the AIDS Confidentiality Act,[96] which had been found to allow "liquidated damages without proof of actual damages."[97]

The *Sekura* court declined to follow the ruling in *Rosenbach*, stating that "we find that the statutory violations to plaintiff's privacy constitute harm even without disclosure" to the defendant's third party vendor, although that disclosure distinguished the case from *Rosenbach* in any event.[98] The *Sekura* court also cited the federal district court decision in *Dixon*, in which the court found that disclosure of fingerprint data to a third party vendor "had alleged an actual injury, specifically 'an injury to a privacy right.'"[99] The plaintiff's claimed mental anguish further distinguished *Sekura* from *Rosenbach*.[100]

IV. *Rosenbach v. Six Flags Entertainment Corp.* in the Illinois Supreme Court

Unanimously reversing the appellate court decision in *Rosenbach*, the Illinois Supreme Court held that the rights protected under BIPA may be enforced in an action for damages and injunctive relief with no showing of any actual damage or injury beyond a bare statutory violation. This holding differed sharply from much of the federal jurisprudence that has arisen since the U.S. Supreme Court's decision in *Spokeo*, with respect to both BIPA claims and claims under other statutes.

91. *Id*. at ¶ 29.
92. *Id*. at ¶¶ 50–55.
93. *Id*. at ¶ 50.
94. *Id*. at ¶ 51.
95. *Id*. at ¶¶ 52–53.
96. AIDS Confidentiality Act, 1987 Ill. Laws 677 (codified as amended in scattered sections of 410 Ill. Comp. Stat. 305) (1987).
97. *Sekura*, 2018 IL App (1st) 180175, ¶¶ 68–71 (citing Doe v. Chand, 335 Ill. App. 3d 809, 822, 781 N.E.2d 340 (Ill. App. Ct. 2002)).
98. *Id*. at ¶ 77.
99. *Id*. at ¶ 80 (quoting Dixon v. Washington & Jane Smith Community–Beverly, No. 17 C 8033, 2018 WL 2445292, at *12 (May 31, 2018)).
100. *Id*. at ¶ 85.

The *Rosenbach* court reached its conclusion through an examination of the language of BIPA, comparing it to other Illinois statutes that included private rights of action. It first noted three decisions that had recently ruled on this issue in the context of BIPA's requirements. On appeal, the Second District of the Illinois Appellate Court ruled in favor of the amusement park, holding that the plaintiff must be "'aggrieved by a violation of the Act,'" and is not aggrieved by alleging "only a technical violation of the Act without alleging any injury of adverse effect."[101] The First District of the Illinois Appellate Court rejected that position in *Sekura*.[102] So had the California federal district court in *In re Facebook Biometric Information Privacy Litigation*.[103] With little further discussion of those decisions, the *Rosenbach* court also rejected that position as the *Facebook* court "correctly reasoned we might do."[104] Notably, the supreme court mentioned neither the *Spokeo* decision nor the concept of Article III standing to sue anywhere in its opinion.

The *Rosenbach* court began its analysis with the "basic principles of statutory construction," with the "primary objective . . . to ascertain and give effect to the legislature's intent."[105] It found "untenable" the defendants' argument that the legislature intended "to limit a plaintiff's right to bring a cause of action to circumstances where he or she has sustained some actual damage, beyond violation of the rights conferred by the statute" because it found that where the Illinois legislature intended to so limit recovery, "it has made that intention clear."[106] The court gave the example of Illinois's Consumer Fraud and Deceptive Business Practices Act,[107] which requires an allegation of actual damage in order to bring a cause of action for damages.[108]

The court contrasted the Consumer Fraud Act's requirement with the AIDS Confidentiality Act, in which "the legislature authorized private rights of action for monetary relief" on merely being "aggrieved" by a violation of the statute, without any proof of actual damages.[109] It found that section 20 of BIPA "clearly follows the latter model."[110] Its conclusion was supported by the fact that BIPA, like the AIDS Confidentiality Act, did not define the term "aggrieved," so that "we assume the legislat[ive] in-

101. Rosenbach v. Six Flags Entm't Corp., 2017 IL App (2d) 170317, ¶ 28, 2017 WL 6523910, at *5 (Ill. App. Ct. Dec. 21, 2017).
102. *Rosenbach*, 2019 IL 123186, ¶ 23,129 N.E.3d 1197, at 1204 (citing *Sekura*, 2018 IL App (1st) 180175).
103. *Id.* (citing *In re* Facebook Biometric Info. Privacy Litig., 326 F.R.D. 535 at 545–47 (N.D. Cal. 2018) (class certification decision)).
104. *Id.*
105. *Id.* at ¶ 24.
106. *Id.* at ¶ 25.
107. 815 Ill. Comp. Stat. 505/10a(a).
108. *Rosenbach*, 2019 IL 123186, ¶ 25.
109. *Id.* at ¶ 26 (citing Doe v. Chand, 335 Ill. App. 3d 809, 822, 781 N.E.2d 840 (Ill. App. Ct. 2002)).
110. *Id.* at ¶ 27.

ten[t] for it to have its popularly understood meaning."[111] Its review of prior case law dealing with the meaning of "aggrieved" persuaded it that a plaintiff is aggrieved if "a legal right is invaded by the act complained of *or* his pecuniary interest is directly affected."[112] Dictionary definitions of "aggrieved" also required no more than that a legal right be infringed or adversely affected.[113]

Looking at what BIPA protects, the *Rosenbach* court found that "our General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information,"[114] and that BIPA's requirements for "the collection, retention, disclosure, and destruction of a person's or customer's biometric identifiers or biometric information define the contours of the statutory right."[115] Failure to comply with the duties imposed by BIPA would clearly make a person "aggrieved" within the meaning of section 20 of the Act and therefore entitled to recover damages.[116]

The court further found that the appellate court's characterization of BIPA violations as merely being "technical" in nature "misapprehends the nature of the harm our legislature is attempting to combat through this legislation" because BIPA was designed to provide individuals "the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent."[117] It concurred with the *Patel* court that "[t]hese procedural protections 'are particularly crucial in our digital world because technology now permits the wholesale collection and storage of an individual's unique biometric identifiers—identifiers that cannot be changed if compromised or misused.'"[118] This conclusion was supported by the legislative statement in section 5(c) of the Act that biometric identifiers bear a "heightened risk" for identity theft if they are compromised.[119]

Finally, the *Rosenbach* court found that the structure of BIPA was designed "to head off such problems before they occur" in two ways.[120] First, the statute imposes a financial penalty "to insure that individuals' and customers' privacy rights in their biometric identifiers and biometric information are properly honored and protected to begin with, before they are or can be compromised."[121] Second, the statute subjects "private entities

111. *Id.* at ¶ 30.
112. *Id.* (quoting Glos v. People, 102 N.E. 763 (1913)).
113. *Id.* at ¶ 32.
114. *Id.* at ¶ 33 (citing Patel v. Facebook, Inc., 290 F. Supp. 3d 948, 953 (N.D. Cal. 2018).
115. *Id.*
116. *Id.*
117. *Id.* at ¶ 34.
118. *Id.* (citing *Patel*, 290 F. Supp. 3d at 954).
119. *Id.* at ¶ 35 (quoting 740 Ill. Comp. Stat. 14/5(c)).
120. *Id.* at ¶ 36.
121. *Id.* (citing 740 Ill. Comp. Stat. 14/20).

who fail to follow the statute's requirements to substantial potential liability, including liquidated damages, injunctions, attorney fees, and litigation expenses 'for each violation' of the law whether or not actual damages, beyond violation of the law's provisions, can be shown."[122]

Weighing the factors involved for those who collect biometric information, the court stated:

> Compliance should not be difficult; whatever expenses a business might incur to meet the law's requirements are likely to be insignificant compared to the substantial and irreversible harm that could result if biometric identifiers and information are not properly safeguarded; and the public welfare, security, and safety will be advanced. That is the point of the law. To require individuals to wait until they have sustained some compensable injury beyond violation of their statutory rights before they may seek recourse, as defendants urge, would be completely antithetical to the Act's preventative and deterrent purposes.[123]

The court therefore declined to "read into the statute conditions or limitations the legislature did not express, and interpret the law in a way that is inconsistent with the objectives and purposes the legislature sought to achieve."[124]

V. The Ninth Circuit's Ruling in *Patel v. Facebook, Inc.*

The Ninth Circuit provided the first major federal court decision on BIPA when it issued its opinion in *Patel v. Facebook, Inc*.[125] on appeal from the *Patel* decision cited by the *Rosenbach* court. In that case, the three named plaintiffs challenged Facebook's "tagging" technology, a software algorithm that enabled the social media platform to use its facial recognition technology to make probable identifications of individuals depicted in photos posted on Facebook. According to the plaintiffs, Facebook's use of its tagging feature to identify individuals in photos constituted an actionable violation of BIPA's restrictions on the use of biometric data. In rejecting Facebook's argument that the lower court erred in certifying a plaintiff class, the court held that "[b]ecause a violation of the Illinois statute injures an individual's concrete right to privacy," the plaintiffs' allegations were sufficient to demonstrate a concrete injury-in-fact for purposes of Article III standing.[126]

First, the *Patel* court explained the history of Facebook's terms and conditions relating to the use of the platform overall, and its use of facial recognition technology. It is only after agreeing to Facebook's terms and conditions, "which permit Facebook to collect and use data in accordance with Facebook's policies," that a Facebook user is permitted to interact with

122. *Id.*
123. *Id.* at ¶ 37.
124. *Id.* at ¶ 38.
125. Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir.), *cert. denied*, No. 19-706 (U.S. Jan. 21, 2020).
126. *Id.* at 1267.

other users on the platform, a number that the court placed at over one billion active users, including roughly seven in ten adults in the United States.[127] The court noted that "[f]or years, Facebook has allowed users to tag their Facebook friends in photos posted to Facebook."[128] These tags include the person's name and a link to their Facebook profile. Although this action was taken by a "friend," and not by the individual tagged, individuals who wished not to be tagged nonetheless had some recourse: "Users who are tagged are notified of the tag, granted access to the photo with other friends, and allowed to share the photo with other friends or 'un-tag' themselves if they choose."[129]

As the *Patel* court noted, Facebook changed the manner in which the tagging feature functioned in 2010 with the launch of "Tag Suggestions," in which control switched from the user to the platform:

> If Tag Suggestions is enabled, Facebook may use facial-recognition technology to analyze whether the user's Facebook friends are in photos uploaded by that user. When a photo is uploaded, the technology scans the photo and detects whether it contains images of faces. If so, the technology extracts the various geometric data points that make a face unique, such as the distance between the eyes, nose and ears, to create a face signature or map. The technology then compares the face signature to faces in Facebook's database of user face templates (i.e., face signatures that have already been matched to the user's profiles). If there is a match between the face signature and the face template, Facebook may suggest tagging the person in the photo.[130]

It was this 2010 change that prompted the plaintiffs' lawsuit. Each of the three named plaintiffs were residents of Illinois, "each uploaded photos to Facebook while in Illinois," and "Facebook created and stored face templates" relating to each of these named class representatives.[131] Based on these facts, the plaintiffs alleged that Facebook violated BIPA by "collecting, using and storing biometric identifiers (a 'scan' of 'face geometry') from their photos without obtaining a written release and without establishing a compliant retention schedule," steps that are required under sections 15(a) and 15(b) of the Illinois law.[132]

In reviewing the plaintiffs' claims, the *Patel* court turned to the language of the statute and its legislative history, noting the key policy statements described above in this article.[133] Quoting the Illinois legislature's statement in the statute, the court stated "[m]oreover, '[t]he full ramifications of biometric technology are not fully known.'"[134] Consequently, it found that

127. *Id.*
128. *Id.*
129. *Id.*
130. *Id.* at 1268.
131. *Id.*
132. *Id.*
133. *See supra* text accompanying note 13.
134. *Id.* at 1269 (quoting 740 Ill. Comp. Stat. 14/5(b)).

"[t]he legislature concluded that '[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.'"[135]

In carrying out its de novo review of the plaintiffs' Article III standing, the *Patel* court reviewed the principles set forth in *Spokeo*, noting that "it is not enough for a plaintiff to allege that a defendant has violated a right created by a statute; we must still ascertain whether the plaintiff suffered a concrete injury-in-fact due to the violation."[136] Noting that "[a] concrete injury need not be tangible," a court's determination of whether an injury meets the *Spokeo* standard of concrete injury-in-fact requires consideration of both history and legislative judgment.[137] The court stated:

> We consider history because "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." We must also examine legislative judgment because legislatures are "well positioned to identify intangible harms that meet minimum Article III requirements."[138]

The Ninth Circuit therefore applied the two-step approach to assessing whether a violation of a statute results in a concrete injury for purposes of Article III standing as articulated in its *Spokeo* remand opinion: We ask "(1) whether the statutory provisions at issue were established to protect [the plaintiffs'] concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests."[139]

In applying that test, the Ninth Circuit looked first at whether BIPA's statutory regime was established to protect concrete interests, as opposed to purely procedural rights. The court harkened back to the seminal Harvard Law Review article in which Samuel Warren and then-future Supreme Court Justice Louis Brandeis articulated the common law right to privacy that would, over time, be recognized as four distinct torts in American jurisprudence.[140] The Ninth Circuit explained that "these common law privacy rights are intertwined with constitutionally protected zones of privacy," and on that basis, found it instructive to examine recent Fourth Amendment jurisprudence as well as claims against private actors alleging an invasion of privacy.[141]

---

135. *Id.*
136. *Id.* at 1270.
137. *Id.*
138. *Id.* (quoting *Spokeo I*, 136 S. Ct. 1540, 1549 (2016)).
139. *Id.* at 1270–71 (quoting *Spokeo II*, 867 F.3d 1108, 1113 (9th Cir. 2017)).
140. *Id.* at 1271–72 (first citing Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 (1890); and then quoting Restatement (Second) of Torts § 652A cmt. a (Am. Law. Inst. 1977)).
141. *Id.* at 1272.

The court cited several Fourth Amendment cases, from *Kyllo v. United States*[142] through *Carpenter v. United States*,[143] in which the Supreme Court recognized the privacy-intrusive impacts of new technology.[144] The court particularly noted the Supreme Court's commentary in *Riley v. California*[145] that "technological advances provide 'access to a category of information otherwise unknowable' and 'implicate privacy concerns' in a manner as different from traditional intrusions as 'a ride on horseback' is different from 'a flight to the moon.'"[146] The Ninth Circuit therefore held that:

> In light of this historical background and the Supreme Court's views regarding enhanced technological intrusions on the right to privacy, we conclude that an invasion of an individual's biometric privacy rights has 'a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.'[147]

It is this portion of the Ninth Circuit's ruling that is perhaps the most significant. In other cases, class action plaintiffs have frequently struggled to demonstrate a concrete injury in cases involving unauthorized sharing or breach of personal information if that information does not fall within the narrowly-drawn confines of traditional state data breach laws or federal data protection laws.[148] Thus, unless the information is likely to lead to a risk of identity fraud or identity theft or other financial harm, many courts have held that there is no cognizable injury that can be recompensed under the law.[149] The *Patel* court made it clear that it views that approach as unduly narrow, observing that, "[a]s in the Fourth Amendment context, the facial-recognition technology at issue here can obtain information that is 'detailed, encyclopedic, and effortlessly compiled,' which would be almost impossible without such technology."[150]

142. Kyllo v. United States, 533 U.S. 27 (2001).
143. Carpenter v. United States, 138 S. Ct. 2206 (2018).
144. *Patel*, 932 F.3d at 1273 (first citing *Kyllo*, 533 U.S. at 34; and then citing *Carpenter*, 138 S. Ct. at 2015).
145. Riley v. California, 573 U.S. 373 (2014).
146. *Patel*, 932 F.3d at 1273 (quoting *Riley*, 573 U.S. at 393).
147. *Id.* (quoting *Spokeo I*, 136 S. Ct. at 1549).
148. *See Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017) (veteran's hospital data breach); Gubala v. Time Warner Cable, Inc., 846 F.3d 909 (7th Cir. 2017) (violations of Cable Communications Policy Act); Braitberg v. Charter Commc'ns, Inc., 836 F.3d 925 (8th Cir. 2016) (same); Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011) (negligence and breach of contract claims for payroll identity theft risks).
149. *See In re* SuperValu, Inc., 925 F.3d 955 (8th Cir. 2019) (grocery store customer information data breach); Katz v. Donna Karan Co., 872 F.3d 114 (2d Cir. 2017) (claims for violations of Fair and Accurate Credit Transactions Act (FACTA)); Crupar-Weinmann v. Paris Baguette Am., Inc., 861 F.3d 76 (2d Cir. 2017) (same).
150. *Patel*, 932 F.3d at 1273 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018)).

The *Patel* court found it significant that, once a face template has been created, Facebook can use it to identify that person in "any of the other hundreds of millions of photos uploaded to Facebook each day," and can deduce from those photos where that person was at particular points in time, and who they were with.[151] The court noted that as the technology continues to advance, Facebook could use the face templates it creates to identify individuals in street or office surveillance photos, or to "unlock the face recognition lock" on an individual's cell phone.[152] Based on both the current and likely future uses of face templates, "[w]e conclude that the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests. Similar conduct is actionable at common law."[153]

The Ninth Circuit further concluded, based on the Illinois Supreme Court's decision in *Rosenbach*, discussed above, that "'the statutory provisions at issue in BIPA' were established to protect an individual's 'concrete interests' in privacy, not merely procedural rights."[154] Accordingly, the court found that the plaintiffs "have alleged a concrete injury-in-fact sufficient to confer Article III standing."[155] It also found that the district court did not abuse its discretion in certifying a plaintiff class.[156] The court has denied Facebook's petition for rehearing en banc,[157] which argued among other things that only substantive violations of BIPA can confer standing and that actual harm is always required to be present.[158] It then stayed its mandate to allow Facebook time to file a petition for certiorari.[159]

Facebook's petition raised the following questions:

1. Whether a court can find Article III standing based on its conclusion that a statute protects a concrete interest, without determining that the plaintiff suffered a personal, real-world injury from the alleged statutory violation.
2. Whether a court can find Article III standing based on a risk that the plaintiff's personal information could be misused in the future, without concluding that the possibility is imminent.
3. Whether a court can certify a class without deciding a question of law that is relevant to determining whether common issues predominate under Rule 23.[160]

151. *Id.*
152. *Id.*
153. *Id.*
154. *Id.* at 1274 (citing *Spokeo II*, 867 F.3d 1108, 1113 (9th Cir. 2017)).
155. *Id.*
156. *Id.* at 1275–77.
157. Order, Patel v. Facebook, Inc., No. 18-15892 (9th Cir. Oct. 18, 2019).
158. Petition for Rehearing En Banc 8–14, Patel v. Facebook, Inc., No. 18-15892 (9th Cir. Sept. 5, 2019).
159. Order, Patel v. Facebook, Inc., No. 18-15892 (9th Cir. Oct. 30, 2019).
160. Petition for Certiorari, Facebook, Inc. v. Patel, No. 19-706 (U.S. Dec. 4, 2019).

Facebook stressed that the plaintiffs could have opted out of the face-tagging feature but did not do so; that they admitted on deposition that "they have suffered no harm from these alleged [BIPA] violations"; that one of the plaintiffs even testified that he liked the feature; and that the plaintiffs had not alleged that "they would have done anything differently, or that their circumstances would have changed in any way" if Facebook had complied with BIPA's notice and consent requirements.[161] It accused the Ninth Circuit of skipping "a fundamental step in the standing analysis," whether each plaintiff had "*in fact* suffered a personal, real-world injury as a result of the alleged statutory violation."[162] Facebook also challenged the Ninth Circuit's failure to determine whether common issues predominated over individual ones on the question of where the alleged BIPA violations occurred, in Illinois or elsewhere.[163]

Facebook argued that the Ninth Circuit's ruling conflicted with rulings in five other circuits that "an alleged statutory violation actually harmed the *plaintiff* 'in a personal and individual way.'"[164] It also argued that the ruling conflicted with four other circuits on the issue of whether future risk of harm must be imminent,[165] compared with only one circuit that agreed that imminence is not required.[166] Facebook pointed out that "*tens of billions of dollars in damages*" were at stake to show the Supreme Court that the issues it presented were "exceptionally important."[167] However, the Court declined to accept Facebook's petition, so these questions were left for the district court to rule on.[168] Facebook chose not to gamble on winning a favorable jury verdict and instead announced a $550 million settlement with the plaintiffs just eight days after its petition for certiorari was denied.[169] This was followed by advising the court of reaching a settlement

161. *Id.* at 5.
162. *Id.*
163. *Id.* at 6.
164. *Id.* at 7 (citing Strubel v. Comenity Bank, 842 F.3d 181, 191 (2d Cir. 2016); Dreher v. Experian Info. Sols., Inc., 856 F.3d 337, 344–47 (4th Cir. 2017); Huff v. TeleCheck Servs, Inc., 923 F.3d 458, 464–69 (6th Cir. 2019); Groshek v. Time Warner Cable, Inc., 865 F.3d 884, 886–89 (7th Cir. 2017); St. Louis Heart Ctr., Inc. v. Nomax, Inc., 899 F.3d 500, 503–05 (8th Cir. 2018)).
165. *Id.* at 7–8 (citing Beck v. McDonald, 848 F.3d 262, 273–75 (4th Cir. 2017); Katz v. Pershing, LLC, 672 F.3d 64, 78–80 (1st Cir. 2012); Reilly v. Ceridian Corp., 664 F.3d 38, 42–44 (3d Cir. 2011); Elec. Privacy Info. Ctr. v. U.S. Dep't of Commerce, 928 F.3d 95, 101–03 (D.C. Cir. 2019)).
166. *Id.* at 7 (citing Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016)).
167. *Id.* at 8–9.
168. Facebook, Inc. v. Patel, 923 F.3d 1260 (9th Cir. 2019), *cert. denied*, No. 19-706 (U.S. Jan. 21, 2020).
169. Allison Grande, *Facebook, Ill. Users Ink Record $550M Biometric Privacy Deal*, Law360 (Jan. 29, 2020), https://www.law360.com/illinois/articles/1238992/facebook-ill-users-ink-record-550m-biometric-privacy-deal?nl_pk=56fa853d-de78-44a4-845b-5d03cb7764e8&utm_source=newsletter&utm_medium=email&utm_campaign=illinois&read_more=1 [https://perma.cc/L96N-PZUK].

in principle four days later.[170] At a hearing on preliminary approval of the class settlement in June 2020, the court reportedly expressed strong disapproval of the amount of the settlement, which would result in class members getting $150 to $300 rather than the $1,000 per violation set by BIPA and would disregard the statute's $5,000 per violation penalty for reckless or willful conduct, which could total up to $47 billion for the class.[171] The court described this as a 99.75% settlement discount. The parties subsequently agreed to increase the settlement to $650 million in July 2020 and the court preliminarily approved the settlement.[172]

VI. The Seventh Circuit's Decision in *Bryant v. Compass Group USA, Inc.*

The Seventh Circuit has weighed in on the Article III standing question in a decision that took an even broader view than the Ninth Circuit took in *Patel*. *Bryant v. Compass Group USA, Inc*.[173] was a purported class action filed in the Circuit Court of Cook County, Illinois by a plaintiff who alleged that the defendant vending machine company violated BIPA in its operation of cashless vending machines at her employer's cafeteria. To use the machines, she set up an account through her employer by submitting fingerprint scans to the defendant, which would use the scans to charge her account for her purchases when she used her fingerprint at the machines.[174] The plaintiff alleged that Compass violated section 15(a) of BIPA because it did not maintain a publicly available retention policy for the biometric identifying information it collected, and that it violated section 15(b) because it provided no written statement that her fingerprints were being collected and stored, it did not state the purpose for their collection or the length of time they would be stored, and it did not obtain her written consent to the collection.[175]

Compass removed the case to federal district court under the Class Action Fairness Act,[176] and the plaintiff then moved to remand the case to

170. Joint Status Report at 2, *In re* Facebook Biometric Information Privacy Litig., No. 3:15-cv-03747-JD (N.D. Cal. Feb. 3, 2020).
171. Dorothy Atkins, Facebook Judge Rips $550 million Biometric Privacy Deal, LAW360.COM (June 5, 2020), https://www.law360.com/illinois/articles/1279996/facebook-judge-rips-550m-biometric-privacy-deal?nl_pk=56fa853d-de78-44a4-845b-5d03cb7764e8&utm_source=newsletter&utm_medium=email&utm_campaign=illinois.
172. Notice of Amended Stipulation of Class Action Settlement at 17, In re Facebook Biometric Information Privacy Litig., No. 3:15-cv-03747-JD (N.D. Cal. July 22, 2020); Order Granting Preliminary Approval of Class Action Settlement, In re Facebook Biometric Information Privacy Litig., No. 3:15-cv-03747-JD (N.D. Cal. Aug. 19, 2020).
173. Bryant v. Compass Group USA, Inc., 958 F.3d 617 (7th Cir. 2020).
174. *Id*. 619.
175. *Id*.
176. 15 U.S.C. § 1332(d) (2018).

state court due to lack of a concrete injury-in-fact necessary to sustain federal subject matter jurisdiction.[177] The district court addressed the question of whether such procedural violations of BIPA, "without any allegation of harm stemming from the violations or any distribution of biometric data to third parties—can constitute concrete injuries for Article III standing purposes."[178] It distinguished the Seventh Circuit's recent BIPA ruling in *Miller v. Southwest Airlines Co*.[179] that found standing to exist in an employee fingerprinting case based on the plaintiff employees' alleged concrete harms in terms of the danger that their fingerprint information might fall into the hands of criminals and that there was a danger that there might be a material change in their terms of employment.[180] Unlike that case, several local district court decisions had found that a BIPA plaintiff does not allege enough concrete harm to sustain jurisdiction "without some additional action by the defendant, like surreptitious collection or disclosure to third parties."[181] The district court also distinguished *Patel* because Facebook's use of the plaintiffs' images "constituted an invasion of their 'private affairs and concrete interests'" and thus provided the necessary concrete harm.[182] Accordingly, following the other district court decisions, the court found that without some allegation of further harm to the plaintiff beyond the bare procedural BIPA violations, she had not sufficiently alleged Article III standing and ordered the case remanded to state court.[183]

Compass was granted leave to appeal, and the Seventh Circuit reversed less than two months after that, holding that "a failure to follow section 15(b) of the law leads to an invasion of personal rights that is both concrete and particularized."[184] The *Bryant* court first remarked on the fact that given the procedural posture of the case, it was the defendant's burden to establish the existence of federal jurisdiction, "a role reversal in the arguments we usually see in these cases, with the defendant insisting that Article III standing is solid, and the plaintiff casting doubt on it."[185] It framed the question before it as whether "any injury she suffered was caused directly by Compass's failure to comply with BIPA, and the prospect of statutory damages shows that such an injury is compensable."[186] Under the Supreme Court's *Spokeo* ruling, where the legislature had acted to "'elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law,'"[187] it was necessary to demonstrate that "'the

177. Bryant v. Compass Group USA, Inc., No. 19-cv-6622, 2020 WL 433868, at *1 (N.D. Ill. Jan. 28, 2020), *rev'd*, 958 F.3d 617 (7th Cir. 2020).
178. *Id*. at *2.
179. Miller v. Southwest Airlines Co., 926 F.3d 898 (7th Cir. 2019).
180. *Bryant*, 2020 WL 433868, at *2.
181. *Id*. at *2–3.
182. *Id*. at *3.
183. *Id*. at *4.
184. *Bryant*, 958 F.3d at 619.
185. *Id*. at 620.
186. *Id*. at 621 (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992).
187. *Id*. (quoting *Spokeo I*, 136 S. Ct. 1548–49).

statutory violation presented an "appreciable risk of harm" to the underlying concrete interest that [the legislature] sought to protect by enacting the statute.'"[188]

Compass argued that the Illinois Supreme Court's decision in *Rosenbach* recognized that the legislature had codified Illinois residents' "right to privacy in and control over their biometric identifiers and biometric information," so that a violation of that right necessarily created "a concrete injury-in-fact for standing purposes."[189] However, given that "standing requirements in Illinois courts are more lenient than those imposed by Article III,"[190] the *Bryant* court could not assume that there was a "perfect overlap between the question before that court and the one before us."[191] It therefore conducted an "independent determination whether the BIPA violations Bryant alleges suffice to support Article III standing."[192]

The *Bryant* court found that it was faced with a matter of first impression because the few federal circuit court of appeals decisions that had addressed standing to sue for BIPA violations had not "decided the precise standing question presented here."[193] In *Miller*, the concrete dangers alleged by the airline workers that caused the district court to distinguish it also caused the Seventh Circuit to do so.[194] The *Bryant* court distinguished *Patel* because the Ninth Circuit "concluded that the common-law right to privacy supplied a concrete interest that was infringed by an 'invasion of an individual's biometric privacy rights,'"[195] and the *Patel* court "also noted that the BIPA provisions at issue were intended 'to protect an individual's 'concrete interests' in privacy, not merely procedural rights."[196] The court also distinguished the Second Circuit's decision in *Santana v. v. Take-Two Interactive Software, Inc*.[197] "because none of the alleged procedural violations raised 'a material risk of harm' to a plaintiff's interest in 'prevent[ing] the unauthorized use, collection, or disclosure of an individual's biometric data'" after the plaintiff had sat for fifteen minutes as his face scan was made.[198] The *Bryant* court found that the many district court cases that required BIPA plaintiffs to allege "some further harm" to establish Article III standing were not binding and also "did not rest on the nature of the

188. *Id*. (quoting Groshek v. Time Warner Cable, Inc., 865 F.3d 884, 887 (7th Cir. 2017).
189. *Id*.
190. *Id*. at 622 (citing Greer v. Illinois Hous. Dev. Auth., 122 Ill. 2d 462, 491, 524 N.E.2d 561 (1988); Duncan v. FedEx Office & Print Servs., Inc., 429 Ill. Dec. 190, 197, 123 N.E.3d 1249 (Ill. App. Ct. 2019); Messenger v. Edgar, 157 Ill. 2d 162, 170, 623 N.E.2d 310 (1993).
191. *Id*.
192. *Id*. at *4.
193. *Id*.
194. *Id*.
195. *Id*. (citing Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019)).
196. *Id*. at 623 (citing *Patel*, 932 F.3d at 1274).
197. 717 F. App'x 12 (2d Cir. 2017).
198. *Bryant*, 958 F.3d at 623.

interest BIPA seeks to protect—personal or public . . . , informational, or formal."[199]

The *Bryant* court drew on "a useful distinction between two types of injuries" discussed in Justice Thomas's concurring opinion in *Spokeo*.[200] One type "arises when a private plaintiff asserts a violation of her own rights; the second occurs when a private plaintiff seeks to vindicate public rights."[201] An action for trespass would fall into the first category, while an action to abate a nuisance would fall into the second.[202] The court found that the plaintiff's BIPA claim under section 15(b) asserted a violation of her own rights in her private fingerprint information, and that "this is enough to show injury-in-fact without further tangible consequences. This is no bare procedural violation; it was an invasion of her private domain, much like an act of trespass would be."[203]

The court went on to consider the BIPA claim as "a type of informational injury" that the Seventh Circuit had dealt with in other cases, usually when information is withheld when the public is entitled to access rather than the opposite situation where BIPA restricts access to information.[204] It found that the plaintiff's claim was analogous to the claim in *Robertson v. Allied Solutions, LLC*,[205] where the defendant employer violated the FCRA by withholding a background report that it relied on to rescind an offer of employment.[206] The *Robertson* plaintiff's "informational injury was both particularized and concrete because she had a 'substantive interest,' protected by FCRA, in being able to 'review the reason for any adverse decision and to respond.'"[207] As in *Robertson*:

> Compass withheld substantive information to which Bryant was entitled and thereby deprived her of the ability to give the *informed* consent section 15(b) mandates. Equipped with the missing information, she may have chosen not to use the vending machines and instead brought her own lunch or snacks. Or she may have opted for the convenience of the machines. She did not realize that there was a choice to be made and what the costs and benefits were for each option. This deprivation is a concrete injury-in-fact that is particularized to Bryant. She thus meets the requirements for Article III standing on her section 15(b) claim.[208]

Further applying Justice Thomas's distinction, the *Bryant* court found that the plaintiff's section 15(a) claim for failure to maintain a publicly

199. *Id.*
200. *Id.* at 624 (citing *Spokeo I*, 136 S. Ct. at 1551 (Thomas, J., concurring)).
201. *Id.* (citing *Spokeo I*, 136 S. Ct. at 1551).
202. *Id.* (citing *Spokeo I*, 136 S. Ct. at 1551–52).
203. *Id.*
204. *Id.* at 624–25.
205. Robertson v. Allied Solutions, LLC, 902 F.3d 690 (7th Cir. 2018).
206. *Bryant*, 958 F.3d at 625.
207. *Id.*
208. *Id.* at 626.

available retention policy for the fingerprint data it collected was "a separate matter."[209] The duty to disclose in that section "is owed to the public generally, not to particular persons whose biometric information the entity collects."[210] The plaintiff lacked standing to pursue that claim because it "is not part of the informed-consent regime" of section 15(b), and the plaintiff had not alleged any concrete and particularized harm arising from the section 15(a) violation.[211]

VII. Biometric Data Protection Under Other State Laws

BIPA was the first statute of its kind that protects biometric data in the United States and arguably remains the strictest. For example, while laws in Texas and Washington have analogous notice and consent requirements,[212] neither of them includes a private right of action for violations of the statutes. The Texas law, which protects biometric identifiers defined as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry,"[213] only provides for an action for a civil penalty not to exceed $25,000 by the Texas attorney general.[214]

The Washington law prohibits any company or individual from entering biometric identifiers "in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose."[215] As in Texas, the Washington statute may only be enforced by the Washington attorney general and contains no private right of action,[216] although it does permit a violation of the law to form the basis of an unfair or deceptive trade practice or unfair competition claim.[217]

The California Consumer Privacy Act (CCPA)[218] went into effect as of January 1, 2020. The CCPA includes biometric data in the definition of protected personal information as comprising "physiological, biological or behavioral characteristics, including [DNA], that can be used . . . to establish individual identity," including "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or

209. *Id.*
210. *Id.*
211. *Id.*
212. Tex. Bus. & Com. Code § 503.001(b); Wash. Rev. Code § 19.375.020(1)–(2) (2013).
213. Tex. Bus. & Com. Code § 503.001(a).
214. *Id.* § 503.001(d).
215. Wash. Rev. Code § 19.375.020(1).
216. *Id.* § 19.375.020(2).
217. *Id.* § 19.375.030(1).
218. California Consumer Privacy Act, 2018 Cal. Legis. Serv. ch. 55 (A.B. 375) (codified at Cal. Civil Code §§ 1798.00-1798.199 (2020)).

rhythms, and sleep, health, or exercise data that contain identifying information."[219] Like BIPA, the CCPA provides a private right of action for certain unauthorized disclosure of biometric information.[220]

New York updated its existing data-breach notification laws with its 2019 Stop Hacks and Improve Electronic Data Security Act (SHIELD Act),[221] effective March 21, 2020, which among other things broadened the definition of protected personal information to include biometric information. The SHIELD Act defines biometric information to include fingerprints, voiceprints, retina or iris images, or other unique physical characteristics and a catchall "other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity."[222] The SHIELD Act requires notification when there is unauthorized access to a New York resident's personal information, including biometric information.[223] Moreover, businesses that maintain the personal information of New York residents must include protections for biometric data when developing and implementing reasonable safeguards as required by the Act.[224] The SHIELD Act expressly confers no private right of action[225] but rather provides for enforcement by the New York attorney general.[226]

Arkansas also recently amended its data breach and response law to include biometric data in the definition of covered personal information. Under the amended statute, biometric data is defined as an individual's "Fingerprints; Faceprint; A retinal or iris scan; Hand geometry; Voiceprint analysis; Deoxyribonucleic acid (DNA); or Any other unique biological characteristics."[227] Under the Arkansas statute, businesses and individuals that acquire, own, or license personal information, including biometric data, are required to implement and maintain reasonable and appropriate security practices to protect the data from unauthorized access or disclosure.[228] In the event of a data breach, businesses and individuals are now required to disclose a security breach of personal information data to affected individuals and, if it affects more than 1,000 persons, to the Arkansas attorney general.[229] Violations of the law can be punishable in action by the attorney general.[230]

219. *Id.* §§ 1798.140(b), 1798.140(o)(1)(E).
220. *Id.* § 1798.150(a)(1).
221. Stop Hacks and Improve Electronic Data Security Act, 2019 N.Y. Sess. Laws ch. 117.
222. N.Y. Gen. Bus. Law § 899-aa.1(b)(5).
223. *Id.* § 899-aa.1(b)(5).
224. *Id.* § 899-aa.2.
225. *Id.* § 899-bb.1(e).
226. *Id.* § 899-bb.1(d).
227. Ark. Code Ann. § 4-110-103(7)(E)(ii)(a)–(g) (2019).
228. *Id.* § 4-110-104.
229. *Id.* § 4-110-105(a)–(b)(2).
230. *Id.* § 4-110-108.

VIII. Conclusion

In denying Facebook's petition for certiorari, the Supreme Court passed on the opportunity to clarify its *Spokeo* decision in situations where statutes provide for damages on a strict liability basis for violations of personal privacy rights, as the Illinois Supreme Court held in *Rosenbach* and the Ninth Circuit held in *Patel*, where the injury may potentially be large but it is not imminent. However, the Seventh Circuit's ruling in *Bryant* that the plaintiff's BIPA claims do satisfy *Spokeo*'s standing requirements for purposes of federal jurisdiction will clearly bolster BIPA plaintiffs' positions by keeping cases filed in or removed to federal district courts pending until they can be addressed on their merits.

The myriad of BIPA cases currently pending in the Northern District of Illinois and elsewhere in the Seventh Circuit will therefore presumably run their course without further consideration of standing to sue under Article III. Federal BIPA cases pending outside of the Seventh and Ninth Circuits may also be affected by the *Bryant* and *Patel* decisions. The very large settlement negotiated in *Patel*, where damages could have run into billions of dollars, just before a trial on the merits seemed inevitable demonstrates forcefully how large a risk defendants run for BIPA violations.[231]

231. *See* Grande, *supra* note 169.