Northern Illinois University Law Review

Volume 42 | Issue 2 Article 6

Spring 5-1-2022

Real Harm in a Virtual World: Establishing Federal Standing in the Seventh Circuit Under Illinois's Biometric Information Privacy Act

Julia Lobo

Real Harm in a Virtual World: Establishing Federal Standing in the Seventh Circuit Under Illinois's Biometric Information Privacy Act

JULIA LOBO[1]

Illinois became the first state to regulate the collection and use of biometric information by private entities when it enacted the Biometric Information Privacy Act in 2008. In the years since, more and more businesses have begun to collect biometric information from their employees and customers. As lawmakers in other states and in Congress look to enact legislation to protect biometric privacy rights, their drafting choices may be informed by three recent Seventh Circuit decisions analyzing when a plaintiff alleging a violation of the Biometric Information Privacy Act has, or has not, established Article III standing as required to proceed in federal court. This Note examines those three closely related decisions: Bryant v. Compass Group USA, Inc., and Fox v. Dakkota Integrated Systems, LLC, both decided in 2020, and Thornley v. Clearview AI, Inc., decided in early 2021.

1. J.D. Candidate, December 2022, Northern Illinois University College of Law.

I. INTRODUCTION

Pay By Touch, a company that deployed fingerprint scanners to process payments in retail locations such as grocery stores and gas stations, filed for bankruptcy in 2007.[2] As the bankruptcy proceedings progressed, an ominous question arose: Would the company's database of more than two million fingerprint scans and associated financial information be sold to the highest bidder?[3] Although the fingerprint database developed by Pay By Touch was ultimately destroyed, the prospect of such a sale prompted the Illinois General Assembly to pass legislation around the collection and use of biometric information.[4]

II. ILLINOIS'S BIOMETRIC INFORMATION PRIVACY ACT

A. SECTION 5 OF THE BIOMETRIC INFORMATION PRIVACY ACT: LEGISLATIVE FINDINGS; INTENT

Illinois enacted the Biometric Information Privacy Act (BIPA) in 2008.[5] The section addressing legislative intent recalls the concerns raised by the Pay By Touch bankruptcy proceedings:

> The General Assembly finds all of the following:
> (a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.
> (b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of bio-

2. Lucy L. Thomson, *Sensitive Personal Data for Sale in Bankruptcy—An Uncertain Future for Privacy Protection*, 2017 NORTONS ANN. SURV. BANKR. L. 12.
3. *Id.*
4. *Id.*
5. 740 ILL. COMP. STAT. 14/1 to 14/99 (2022).

> metric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.[6]

This section of the law closes with two observations that still ring true more than a decade later, and which speak to the need for heightened protections around biometric information. Subsection 5(f) notes that "[t]he full ramifications of biometric technology are not fully known," and subsection 5(g) goes on to state 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."[7]

B. SECTION 10 OF THE BIOMETRIC INFORMATION PRIVACY ACT: DEFINITIONS

BIPA protects more than just fingerprints. The law defines biometric information as "any information . . . based on an individual's biometric identifier used to identify an individual."[8] And "biometric identifier," as defined in the text of BIPA, refers to "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[9]

BIPA's regulations and restrictions only apply to "private entities."[10] A private entity is defined in section 10 as "any individual, partnership, corporation, limited liability company, association, or other group, however organized."[11] State or local government agencies are specifically excluded from BIPA's reach, as are "any court of Illinois, a clerk of the court, or a judge or justice thereof."[12]

C. SECTION 15 OF THE BIOMETRIC INFORMATION PRIVACY ACT: RETENTION; COLLECTION; DISCLOSURE; DESTRUCTION

Section 15 contains the heart of the privacy regulations.[13] Subsection 15(a) requires "a written policy, made available to the public" that establishes the private entity's schedule for the retention and destruction of biometric information.[14] The destruction of the biometric information must occur as soon as the purpose of the collection has been satisfied, or within

---

6. 740 ILL. COMP. STAT. 14/5 (2022).
7. *Id.*
8. 740 ILL. COMP. STAT. 14/10 (2022).
9. *Id.*
10. *See* 740 ILL. COMP. STAT. 14/15 (2022).
11. 740 ILL. COMP. STAT. 14/10 (2022).
12. *Id.*
13. 740 ILL. COMP. STAT. 14/15 (2022).
14. 740 ILL. COMP. STAT. 14/15(a) (2022).

three years from the entity's last interaction with the individual, whichever occurs first.[15] Under 15(a), the entity must also *comply* with its written policy, unless the biometric information is the subject of a warrant or subpoena.[16]

Subsection 15(b) sets out requirements for informed consent.[17] First, the private entity must notify the individual in writing that it is collecting biometric information.[18] Second, it must notify the individual of the specific purpose of the collection, as well as the length of time for which the information will be stored and used.[19] Third, the entity must obtain written consent from the individual prior to collecting the information.[20]

Subsection 15(d) outlines restrictions on the disclosure and dissemination of biometric information,[21] while subsection 15(e) requires private entities to use a "reasonable standard of care" in protecting any biometric information in its possession.[22] The measures used to protect biometric information must be "the same as or more protective than the manner in which the private entity . . . protects other confidential and sensitive information."[23]

D. SECTION 20 OF THE BIOMETRIC INFORMATION PRIVACY ACT: RIGHT OF ACTION

Section 20 of BIPA gives the law its teeth. This section reads:

> **§ 20. Right of action.** Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:
> (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;
> (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

15. *Id.*
16. *Id.*
17. 740 ILL. COMP. STAT. 14/15(b) (2022).
18. 740 ILL. COMP. STAT. 14/15(b)(1) (2022).
19. 740 ILL. COMP. STAT. 14/15(b)(2) (2022).
20. 740 ILL. COMP. STAT. 14/15(b)(3) (2022).
21. 740 ILL. COMP. STAT. 14/15(d) (2022).
22. 740 ILL. COMP. STAT. 14/15(e) (2022).
23. *Id.*

> (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
> (4) other relief, including an injunction, as the State or federal court may deem appropriate.[24]

This brief section of the law has given rise to many of the disputes around BIPA. For example, what exactly does "aggrieved" mean? And how might a plaintiff be aggrieved? Though the legislation was enacted in 2008, these remained open questions for Illinois courts until 2019, when the state's supreme court ruled on a BIPA plaintiff's standing to sue.

III. *ROSENBACH*: THE LANDMARK CASE

A. THE ILLINOIS SUPREME COURT ADDRESSES STANDING REQUIREMENTS FOR BIPA COMPLAINTS

In *Rosenbach v. Six Flags Entertainment Corp.*, Six Flags Great America theme park in Gurnee, Illinois, had taken the thumbprint of a 14-year-old boy as part of its standard procedure for issuing season passes.[25] Because the theme park failed to obtain informed consent as required by section 15(b) of BIPA, the boy's mother filed a complaint seeking damages for the statutory violation as well as injunctive relief to ensure that the theme park would obtain informed consent before collecting biometric information in the future.[26]

Six Flags filed a motion to dismiss the complaint, arguing that the plaintiff "had suffered no actual or threatened injury and therefore lacked standing to sue."[27] The Illinois trial court denied the motion to dismiss.[28] The appellate court granted the defendant's request for review and held that the plaintiff did not have standing to sue "based solely on a defendant's violation of the statute. Additional injury or adverse effect must be alleged."[29] The plaintiff then appealed to the Illinois Supreme Court.[30]

In a unanimous decision, the Illinois Supreme Court reversed the appellate court, ruling that the plaintiff did have standing to sue for the defendant's BIPA violations.[31] In reaching this conclusion, the court looked to

---

24. 740 ILL. COMP. STAT. 14/20 (2022).
25. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1200, 2019 IL 123186, ¶¶ 5-7.
26. *Id.* at 1201.
27. *Id.* at 1201-02.
28. *Id.* at 1202.
29. *Id.*
30. *Rosenbach*, 129 N.E.3d at 1202.
31. *Id.* at 1199-1200; *see also id.* at 1207.

the plain language of the statute in order to ascertain the legislature's intent.[32] The court stated that when a statutory term is not defined within the statute, as is the case with BIPA's use of the term *aggrieved*, the court will assume that "the legislature intended for it to have its popularly understood meaning."[33] In addition, the court will look to the "settled legal meaning" of the term.[34] And in this case, both of these approaches supported Rosenbach's understanding of *aggrieved*.[35]

Quoting a 1913 Illinois Supreme Court decision, the court stated that a person is "aggrieved, in the legal sense, when a legal right is invaded by the act complained of."[36] Because that definition has since been so widely repeated by Illinois courts, the court said that it "must presume that the legislature was aware of that precedent and acted accordingly."[37]

This definition is consistent with the popular understanding of the term. For example, one definition of *aggrieved* offered by Merriam-Webster's Collegiate Dictionary is "suffering from an infringement or denial of legal rights."[38] Likewise, Black's Law Dictionary defines *aggrieved* as "having legal rights that are adversely affected."[39] Based on these dictionary definitions, the court again concluded that the legislature intended to invoke this meaning when drafting the Biometric Information Privacy Act.[40]

By enacting BIPA, the Illinois legislature established that individuals have a right to privacy in their biometric information.[41] Therefore, when a company fails to comply with the requirements of BIPA, the company violates those privacy rights, and an affected individual is aggrieved and entitled to file suit under BIPA's private right of action.[42]

Furthermore, the idea that an individual could not file suit under BIPA in the absence of actual damages is inconsistent with BIPA's goal of preventing that sort of damage from occurring in the first place. Here, the court pointed to the fact that the Illinois legislature "expressly noted that '[b]iometrics are unlike other unique identifiers . . . For example, social security numbers, when compromised, can be changed. Biometrics, howev-

---

32. *Id.* at 1204.
33. *Id.* at 1205.
34. *Rosenbach*, 129 N.E.3d at 1205.
35. *Id.*
36. *Id.* (quoting Glos v. People, 102 N.E. 763, 766 (Ill. 1913)).
37. *Id.*
38. *Id.* (quoting *Aggrieved*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2006)).
39. *Rosenbach*, 129 N.E.3d at 1205 (quoting *Aggrieved*, BLACK'S LAW DICTIONARY (9th ed. 2009)).
40. *Id.*
41. *Id.*
42. *Id.*

er, are biologically unique to the individual; therefore, once compromised, the individual has no recourse.'"[43] How does BIPA seek to prevent this irreversible damage? In two ways: First, by erecting safeguards around individuals' privacy rights related to biometric information.[44] Second, by imposing substantial potential liabilities on private entities who fail to comply with the requirements of BIPA.[45]

In fact, "[o]ther than the private right of action . . . no other enforcement mechanism is available."[46] And because BIPA can protect biometric information privacy only if private entities have a strong incentive to follow the law, the legislature must have meant for the private right of action "to have substantial force."[47] The court expanded on this point, saying that

> [c]ompliance 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.[48]

In *Rosenbach*, the Illinois Supreme Court established that, in Illinois courts, a plaintiff "need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act."[49]

---

43. *Id.* (quoting 740 ILL. COMP. STAT. ANN. 14/5(c) (West 2016)).
44. *Rosenbach*, 129 N.E.3d at 1206-07. *See* 740 ILL. COMP. STAT. 14/15 (2022).
45. *Rosenbach*, 129 N.E.3d at 1207. *See* 740 ILL. COMP. STAT. 14/20 (2022).
46. *Rosenbach*, 129 N.E.3d at 1207.
47. *Id.*
48. *Id.*
49. *Id.*

B. *ROSENBACH* AMICI BRIEF: ACLU ET AL. ARGUE FOR PLAINTIFF'S STANDING TO SUE

When the Illinois Supreme Court accepted the *Rosenbach* case for review, it also accepted "friend of the court" briefs in support of both the plaintiff and the defendant.[50] The amici brief submitted by the American Civil Liberties Union ("ACLU") et al. explained that the ACLU, along with the ACLU of Illinois, had drafted BIPA and had been "instrumental to its passage."[51] The brief urged the Illinois Supreme Court to hold that Rosenbach did have standing to sue in Illinois state court, arguing that, if the court found she did not have standing, the ruling would "significantly undermine the private enforcement mechanism of the statute, . . . leaving no means to hold wrongdoers accountable for their violations of BIPA's notice and consent requirements."[52]

The ACLU's brief stressed the importance of enforcing BIPA's protections for individuals in the face of dangers such as the surreptitious collection of biometric data, particularly as related technologies continue to advance.[53] For example, at the time the brief was written, the technology already existed to "conduct iris scans at a distance of up to 12 meters, eliminating the need for people to place their eye directly in front of an eye-scanning camera or even to be aware that the scanning is taking place."[54] Illinois residents would be protected from such invasive and clandestine practices only if BIPA's requirements for notice could be effectively enforced.[55]

And while the data collection at issue in the *Rosenbach* case was not surreptitious, it occurred in the type of "functionally nonvoluntary" context contemplated by the legislators who enacted BIPA.[56] The requirement for informed consent ensures not only that individuals are aware that biometric information is being collected, but also that they are made aware of the terms of that collection prior to surrendering their biometric information.[57] A violation of BIPA's notice and consent requirements impairs an individual's ability to protect and control personal biometric data and therefore

---

50. *Id.* at 1202.

51. Brief for ACLU et al. as Amici Curiae Supporting Plaintiff-Appellant, Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197 (Ill. 2019), (No. 123186), 2018 WL 577921.

52. *Id.* at 4.

53. *Id.* at 8.

54. *Id.* at 7.

55. *Id.* at 8.

56. Brief for ACLU et al. as Amici Curiae Supporting Plaintiff-Appellant at 16, Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 2019 IL 123186 (No. 123186), 2018 WL 5777921.

57. *Id.*

"creates an actionable privacy harm."[58] In other words, a violation of BIPA's substantive requirements is not merely a bare procedural violation; rather, "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*."[59]

C. *ROSENBACH* AMICUS BRIEF: THE ILLINOIS CHAMBER OF COMMERCE ARGUES AGAINST PLAINTIFF'S STANDING TO SUE

The Illinois Chamber of Commerce ("Chamber"), an advocate for Illinois businesses, authored one of the briefs filed in support of Six Flags.[60] In its brief, the Chamber warned that, should the Illinois Supreme Court hold that Rosenbach had standing to sue, similar complaints seeking "catastrophic damages" would drive businesses "either out of Illinois or into bankruptcy," thereby damaging the state's economy.[61]

The Chamber argued that complaints such as Rosenbach's sought to impose "strict-liability on Illinois businesses for technical violations of BIPA," which would allow plaintiffs to sue in the absence of harm, and that "the result would be devastating to Illinois businesses."[62] The Chamber urged the court to instead uphold the appellate court's ruling that a plaintiff "must allege some actual harm" in order to sue for a violation of BIPA.[63] As stated in the *Rosenbach* decision from the Illinois Appellate Court for the Second District, "[i]f a person alleges only a technical violation of the Act without alleging any injury or adverse effect, then he or she is not aggrieved and may not recover under any of the provisions" of BIPA.[64]

In contrast to the ACLU's argument that BIPA was intended to create robust privacy protections for individuals, the Chamber construed the purpose of the legislation more narrowly. The Chamber quoted a decision from the Southern District of New York, which stated that BIPA was meant "to ensure that, when an individual engages in a biometric-facilitated transaction, the private entity protects the individual's biometric data, and does not use that data for an improper purpose, especially a purpose not contemplat-

---

58. *Id.* at 11.

59. *Id.* at 17 (quoting Patel v. Facebook, Inc., 290 F. Supp. 3d 948, 954 (N.D. Cal. 2018)).

60. Brief for Amicus Curiae Illinois Chamber of Commerce Supporting Defendants-Appellees, Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 2019 IL 123186 (No. 123186), 2018 WL 5777926.

61. *Id.* at 1-2.

62. *Id.* at 1.

63. *Id.* at 2.

64. *Id.* at 4 (quoting Rosenbach v. Six Flags Ent. Corp., 147 N.E.3d 125, 131, 2017 IL App (2d) 170317, ¶ 28).

ed by the underlying transaction."[65] Or, as stated by the Chamber, BIPA was enacted to guard against "the improper disclosure and sale of consumers' biometric data — not to impose strict liability on Illinois businesses."[66]

The Chamber went on to argue that reversing the appellate court's decision in *Rosenbach* would "open the floodgates for future litigation" and create an existential threat to small businesses in Illinois.[67] While biometric technology is often utilized by Illinois businesses so that employees cannot clock in or clock out for coworkers, those same companies lack the financial resources to survive BIPA lawsuits.[68]

Next, the Chamber turned to the potentially "devastating damages" that could be obtained by plaintiffs for BIPA violations.[69] While section 20 of BIPA lists damages at a minimum of $1,000 for each negligent violation and $5,000 for each reckless violation of the Act, damages could quickly escalate if each and every fingerprint scan counted as a violation.[70] For example, an employee might use a fingerprint scanner four times a day: clocking in at the start of the day, clocking out for lunch, clocking in after lunch, and then clocking out for the day.[71] In addition, the Chamber said, plaintiffs in class action suits have sought to apply a five-year statute of limitations (the "catch-all" statute of limitations in Illinois) because BIPA does not list its own statute of limitations.[72]

The Chamber went on to calculate potential damages for companies of various sizes.[73] Assuming $1,000 per violation, with each employee scanning a fingerprint four times a day while working five days a week, fifty weeks a year, for five years, companies would owe $5 million per employee.[74] A company with twenty employees could be faced with $100 million in damages, while a company with 1,000 employees would face $5 billion in damages.[75] The Chamber then concluded that "many Illinois businesses

65. Brief for Amicus Curiae Illinois Chamber of Commerce Supporting Defendants-Appellees, *supra* note 60, at 3 (quoting Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 520 (S.D.N.Y. 2017)).

66. *Id.* at 2.

67. *Id.* at 4-5.

68. *Id.* at 5-6.

69. *Id.* at 8.

70. Brief for Amicus Curiae Illinois Chamber of Commerce Supporting Defendants-Appellees, *supra* note 60, at 8-9.

71. *Id.* at 9.

72. *Id.*

73. *Id.* at 10.

74. *Id.*

75. Brief of Amicus Curiae Illinois Chamber of Commerce in Support of Defendants-Appellees at 10, Rosenbach v. Six Flags Ent. Corp., (Ill. 2019) (No. 123186), 2018 WL 5777926.

may be forced to settle for significant amounts," which in turn would harm the state's economy, "to the ultimate detriment of all Illinois residents."[76]

IV. CLEARVIEW AI: BIOMETRIC PRIVACY CONCERNS IN THE NATIONAL SPOTLIGHT

The Illinois Supreme Court ruled on the *Rosenbach* case in January 2019. A year later, in January 2020, the *New York Times* put biometric privacy concerns in the national spotlight with the publication of an article titled "The Secretive Company That Might End Privacy As We Know It."[77] While the Pay By Touch bankruptcy raised the possibility of a private company profiting from biometric information, this article showed that, more than a decade later, it had become a reality. The article focused on a little-known company called Clearview AI, which had provided both clients and potential clients with access to its "groundbreaking facial recognition app" that allows users to upload a photo of an unidentified person and run it through a database of more than three billion images to find potential matches.[78] Clearview created the breathtakingly vast database, which "goes far beyond anything ever constructed by the United States government or Silicon Valley giants," by collecting photos of faces along with identifying information from "Facebook, YouTube, Venmo and *millions of other websites*."[79]

When *New York Times* analysts reviewed the computer code behind the Clearview app, they uncovered "programming language to pair [the app] with augmented-reality glasses," suggesting that Clearview clients might someday be able to surreptitiously identify nearly any person on the street, such as "activists at a protest or an attractive stranger on the subway, revealing not just their names but where they lived, what they did and whom they knew."[80]

Who might be on Clearview's list of clients? According to Clearview, the Indiana State Police became its first customer in February 2019.[81] And in the year that followed, more than six hundred law enforcement agencies joined the client list, including the Federal Bureau of Investigation and the

---

76. *Id.* at 11-12.

77. Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, N.Y. TIMES (updated Feb. 10, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/B77H-QJUW].

78. *Id.*

79. *Id.* (emphasis added). Note that "Facebook and other social media sites prohibit people from scraping users' images — Clearview is violating the sites' terms of service." *Id.*

80. *Id.*

81. Hill, *supra* note 77.

Department of Homeland Security.[82] The following anecdote demonstrates the app's utility for law enforcement agencies:

> [The Indiana State Police] solved a case within 20 minutes of using the app. Two men had gotten into a fight in a park, and it ended when one shot the other in the stomach. A bystander recorded the crime on a phone, so the police had a still of the gunman's face to run through Clearview's app. [The police] immediately got a match: The man appeared in a video that someone had posted on social media, and his name was included in a caption on the video. "He did not have a driver's license and hadn't been arrested as an adult, so he wasn't in government databases," said Chuck Cohen, an Indiana State Police captain at the time. The man was arrested and charged; Mr. Cohen said he probably wouldn't have been identified without the ability to search social media for his face.[83]

In addition to an immense database of potential matches, Clearview offers facial recognition technology that is more robust than government-issued facial recognition software. For example, the app can find a match even if the suspect is wearing a hat or glasses, or isn't looking toward the camera.[84]

Soon after the publication of the *New York Times* article, BuzzFeed News reported that Clearview had provided its services (or at least a free trial) to employees at more than two hundred private companies, including Walmart, Best Buy, and Wells Fargo.[85] The client log reviewed by BuzzFeed listed Macy's department store, for example, as a paying customer with more than six thousand searches conducted through its account, placing Macy's among the private companies with the most searches.[86]

---

82. *Id.*
83. *Id.*
84. *Id.*
85. Ryan Mac et al., *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED NEWS (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement [https://perma.cc/DK52-GYWJ].
86. *Id.*

BuzzFeed later reported that Macy's had terminated its contract with Clearview AI in January 2020, according to a company spokesperson.[87]

The *New York Times* article didn't just bring media attention to this "secretive company"; in addition, a "rash of lawsuits followed in the wake of the article."[88] By May 2020, Clearview found itself fighting a motion for a preliminary injunction in *Mutnick v. Clearview AI, Inc*.[89] In its motion filed with the United States District Court in the Northern District of Illinois, Clearview outlined the ways it had voluntarily taken steps to comply with the requirements of BIPA.[90]

Arguing that its voluntary actions rendered the request for an injunction moot, Clearview stated that it had "recently and voluntarily changed its business practices to avoid including data from Illinois residents and to avoid transacting with non-governmental customers anywhere."[91] The company went on to say that it was "cancelling the accounts of every customer who was not either associated with law enforcement or some other federal, state, or local government department, office, or agency . . . [and] all accounts belonging to any entity based in Illinois."[92] In addition, the company stated that it had taken steps to block access "to Illinois Information until the conclusion of these litigations" and had updated its terms of use to prohibit "users from uploading images of Illinois residents."[93]

V. BIPA PROTECTIONS AND CONCRETE INJURIES: THE QUESTION OF FEDERAL STANDING REACHES THE SEVENTH CIRCUIT

When BIPA took effect in 2008, Illinois became the first state in the country to regulate issues around biometric information privacy.[94] Howev-

87. Ryan Mac et al., *Clearview AI Has Promised to Cancel All Relationships With Private Companies*, BUZZFEED NEWS (May 7, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies [https://perma.cc/8E4Z-E2AN].

88. Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1243 (7th Cir. 2021) (providing background for defendant, Clearview AI, Inc.). "See, *e.g., Mutnick v. Clearview AI, Inc.*, No. 1:20-cv-00512 (N.D. Ill.); *Roberson v. Clearview AI, Inc.*, No. 1:20-cv-00111 (E.D. Va.); *Calderon v. Clearview AI, Inc.*, No. 1:20-cv-01296 (S.D.N.Y.); *Burke v. Clearview AI, Inc.*, No. 3:20-cv-00370 (S.D. Cal.). This case was one of them." *Id.*

89. Clearview Defendants' Memorandum of Law in Opposition to Plaintiff's Motion for Preliminary Injunction, Mutnick v. Clearview AI, Inc., No. 20-cv-512 (N.D. Ill. May 6, 2020).

90. *Id.* at 1.

91. *Id.* at 3.

92. *Id.*

93. *Id.* at 6-7.

94. JOHN M. FITZGERALD, GUIDE TO THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT 5-6 (2020).

er, the new legislation was largely ignored for the next seven years.[95] It was not until December 2015 that a reported judicial decision addressed a BIPA complaint.[96] Since then, BIPA has become "arguably the fastest-growing and most-discussed area of civil litigation in Illinois," and has led to "massive class action litigation in far-flung parts of the country."[97] With plaintiffs filing BIPA complaints in Illinois state courts, only to have cases removed to federal court by defendants, it wasn't long before federal courts were put in the unusual position of hearing plaintiffs argue that they lacked federal standing, while defendants asserted that the standing requirements were satisfied. Three such cases are discussed below.

A. *BRYANT V. COMPASS GROUP USA, INC.*

In *Bryant v. Compass Group USA, Inc.*, a call center in Illinois installed vending machines owned by Compass Group USA, Inc. ("Compass") in its employee cafeteria.[98] The vending machines relied on pay-by-touch technology, scanning a fingerprint to deduct funds from a linked account, and did not accept cash.[99] During orientation at the call center, Christine Bryant and other new hires were instructed to submit scans of their fingerprints and create user accounts for the vending machines.[100] Compass did not have publicly available policies for the retention and destruction of the fingerprints scans, as required by section 15(a) of BIPA.[101] Nor did Compass obtain informed consent from Bryant, as required by section 15(b) of BIPA.[102] Although Bryant scanned her fingerprint and used the vending machines voluntarily, Compass's failure to comply with BIPA meant that she lost the opportunity to make an informed decision as to whether or not to give Compass control of her biometric information.[103]

Bryant filed a complaint against Compass in the Cook County Circuit Court.[104] Because the complaint was a putative class action, Compass used the Class Action Fairness Act to remove the case to federal court on the

---

95. *Id.* at 5.
96. *Id.* (citing Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103 (N.D. Ill. 2015)).
97. *Id.* (citing, *e.g.*, Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019)). This class action ultimately settled for $650 million. *See* Robert Channick, *Nearly 1.6 Million Illinois Facebook Users to Get About $350 Each in Privacy Settlement*, CHI. TRIB. (Jan. 14, 2021, 8:04 PM), https://www.chicagotribune.com/business/ct-biz-facebook-privacy-settlement-illinois-20210115-2gau5ijyjff4xd2wfiiow7yl4m-story.html.
98. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617, 619 (7th Cir. 2020).
99. *Id.*
100. *Id.*
101. *Id.*
102. *Id.*
103. *Bryant*, 958 F.3d at 620.
104. *Id.*

basis of diversity of citizenship and amount in controversy.[105] Bryant then asserted that, "because she lacked the concrete injury-in-fact necessary to satisfy the federal requirement for Article III standing," the case should be remanded to state court.[106] The federal district court sided with Bryant, ruling that the complaint alleged "bare procedural violations," which were insufficient to establish federal standing.[107] The Northern District of Illinois remanded the case to state court and Compass appealed.[108]

The Seventh Circuit accepted the appeal, noting in its decision that, "[a]s the party invoking federal jurisdiction, Compass bears the burden of establishing Bryant's Article III standing . . . . This fact has occasioned a role reversal in the arguments we normally see in these cases, with the defendant insisting that Article III standing is solid, and the plaintiff casting doubt on it."[109] The court then went on to identify the central issue: "For Bryant to have Article III standing . . . she must have suffered an actual or imminent, concrete and particularized injury-in-fact."[110] Citing the 2016 Supreme Court decision in *Spokeo, Inc. v. Robins*, the court further explained that an injury can be concrete even if it is intangible.[111]

Compass argued that the *Rosenbach* decision, although it addressed a plaintiff's standing only in Illinois state court, supports an argument for federal standing as well.[112] Rosenbach had a right to control and protect the biometric information that had been gathered, a right which the Illinois General Assembly sought to protect by passing BIPA.[113] Because a violation of BIPA is a violation of those rights, Bryant, like Rosenbach, suffered a "real and significant" injury.[114]

While acknowledging that the reasoning in *Rosenbach* may be helpful, the Seventh Circuit stated that "we cannot uncritically assume perfect overlap between the question before the state court and the one before us."[115] The court went on to explain that, although both federal courts and Illinois courts require an "injury in fact," Illinois courts define the term differently, and, as a result, standing requirements in Illinois courts are not as stringent as federal requirements for Article III standing.[116]

---

105. *Id.*
106. *Id.*
107. *Id.*
108. *Bryant*, 958 F.3d at 620.
109. *Id.*
110. *Id.* at 620-21.
111. *Id.* at 621 (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).
112. *Id.* at 621.
113. *Bryant*, 958 F.3d at 621.
114. *Id.* at 621-22.
115. *Id.* at 622.
116. *Id.*

The court then turned to three previous federal circuit court decisions in BIPA cases, noting that "none has decided the precise standing question presented here."[117] The Seventh Circuit, in its 2019 decision in *Miller v. Southwest Airlines Co.*, had held that union airline workers who had been required to clock in and clock out with fingerprint scans had federal standing for complaints alleging violations of BIPA sections 15(a) and 15(b).[118] The Ninth Circuit, in its 2019 decision in *Patel v. Facebook, Inc.*, had found that plaintiffs had alleged an injury-in-fact by claiming that Facebook violated BIPA when it deployed facial-recognition technology without users' informed consent.[119] In 2017, a nonprecedential summary order from the Second Circuit had gone the other way.[120] In *Santana v. Take-Two Interactive Software, Inc.*, where the plaintiff had explicitly consented to the facial scan used to create a personalized game avatar, but the defendant had failed to include every term required by BIPA for *informed* consent,[121] the Second Circuit reasoned that the plaintiff lacked federal standing because the "procedural violations" of BIPA did not create "a material risk of harm" to the plaintiff's privacy interests.[122] In addition, the Second Circuit noted that the parties' arguments over federal standing were "based on differing constructions of the term 'aggrieved party' as used in BIPA,"[123] a reminder that the *Santana* decision predated the Illinois Supreme Court's *Rosenbach* decision.

Next, the court listed BIPA cases that had been decided in the Northern District of Illinois, stating that "[t]he majority of the district courts in this circuit have rejected standing for plaintiffs alleging only violations of sections 15(a) and (b), without some further harm."[124] The Seventh Circuit observed that it was not bound by the district court decisions, and also noted that those decisions "did not rest on the nature of the interest BIPA seeks to protect" and that, therefore, *Bryant* presented "a question of first impression."[125]

To answer this question, the court began by taking a closer look at the *Spokeo* case because it "provides substantial guidance about cases alleging

---

117. *Id.*

118. *Bryant*, 958 F.3d at 622 (citing Miller v. Southwest Airlines Co., 926 F.3d 898 (7th Cir. 2019)).

119. *Id.* (citing Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019)).

120. *Id.* at 623 (citing Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 14 (2d Cir. 2017)).

121. Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12, 14 (2d Cir. 2017).

122. *Id.* at 15.

123. *Id.* at 17.

124. *Bryant*, 958 F.3d at 623.

125. *Id.*

the kind of intangible harm to personal interests that Bryant asserts."[126] In *Spokeo*, the plaintiff alleged injuries caused by inaccuracies in his personal information reported by a "people search engine."[127] The federal district court dismissed his complaint, ruling that he lacked Article III standing.[128] The Ninth Circuit reversed the decision, and the Supreme Court later accepted the case for review.[129]

The Supreme Court ultimately did not decide whether or not the plaintiff in *Spokeo* had established federal standing; the Court ruled only that the Ninth Circuit had used the wrong standard in its analysis.[130] The Ninth Circuit's analysis had focused on whether the plaintiff had suffered a particularized harm, which the Supreme Court held was necessary but not sufficient.[131] To establish standing, the plaintiff's injury needed to be both particularized and concrete.[132] The Court went on to explain that "[a]lthough tangible injuries are perhaps easier to recognize . . . intangible injuries can nevertheless be concrete," and that "the *risk* of real harm can suffice, and injury-in-fact is not defeated just because the injury is 'difficult to prove or measure.'"[133]

For further guidance, the Seventh Circuit looked to Justice Thomas's concurrence in *Spokeo*, where he drew a distinction between complaints that allege a violation of the plaintiff's own rights (e.g., trespass or infringements on intellectual property) and complaints that allege a violation of the rights of the public (e.g., public nuisance or disputed use of public land).[134] The Seventh Circuit then concluded that Bryant's complaint alleged "an invasion of her private domain, much like an act of trespass," and that this invasion was sufficient to establish injury-in-fact, as required by Article III.[135]

The Seventh Circuit stated that, alternatively, Bryant's standing could be established by viewing her alleged injuries as "a type of informational injury."[136] Under this analysis, the key issue is whether "the plaintiff is entitled to receive and review *substantive* information."[137] Applying this standard to the *Bryant* case, the court held that standing would be established

126. *Id.* (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).
127. *Id.* (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).
128. *Id.* (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).
129. *Bryant*, 958 F.3d at 623 (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).
130. *Id.* (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).
131. *Id.* at 624 (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).
132. *Id.* (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).
133. *Id.* (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).
134. *Bryant*, 958 F.3d at 624 (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).
135. *Id.*
136. *Id.*
137. *Id.* at 625 (quoting Robertson v. Allied Sols., LLC, 902 F.3d 690, 697 (7th Cir. 2018)).

based on "the substantive and personal nature of the information Compass was obligated under BIPA to disclose to consumers such as Bryant."[138] By enacting section 15(b) of BIPA, the Illinois General Assembly sought to protect highly sensitive personal information by ensuring that individuals would "be given the opportunity to make informed choices about to whom and for what purpose" they would share their biometric information.[139] By failing to comply with section 15(b), Compass denied Bryant the opportunity to weigh the potential risks against the conveniences of sharing her fingerprint with the company.[140] Depriving Bryant of her right to make an informed decision amounts to an injury that is both concrete and particularized, as required for Article III standing.[141]

Having determined that Bryant had federal standing for her claim related to section 15(b), which the court identified as "the heart of BIPA," the court then turned to a different issue—whether Bryant had federal standing for her claim related to section 15(a).[142] Because Bryant's complaint cited only the first half of section 15(a) (which requires companies to have a publicly available policy for retention and destruction of biometric information), the court did not include in its analysis the second half of 15(a) (which requires companies to comply with those publicly available policies).[143]

Importantly, Bryant's claim related to section 15(a) alleged the breach of a duty owed to the general public, and she did not allege any particularized harm.[144] Therefore, the court quickly concluded that Bryant's section 15(a) claim had not alleged a concrete, particularized injury, and so she did not have Article III standing for that portion of her complaint. The court went on to state that it had "no authority and no occasion to address her state-court standing" for the claim under section 15(a).[145]

B. *FOX V. DAKKOTA INTEGRATED SYSTEMS, LLC*

The Seventh Circuit affirmed and further clarified the *Bryant* holding regarding federal standing for section 15(a) claims in *Fox v. Dakkota Integrated Systems, LLC*.[146] Fox had sued her former employer in state court for alleged BIPA violations stemming from the employer's requirement that

138. *Id.* at 626.
139. *Bryant*, 958 F.3d at 626.
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *Bryant*, 958 F.3d at 626.
145. *Id.*
146. Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146 (7th Cir. 2020).

employees clock in and clock out by placing a hand on a biometric scanner.[147] The defendant employer removed the proposed class action suit to federal court where the judge remanded the section 15(a) claim to state court, citing the Seventh Circuit's *Bryant* decision.[148]

The Seventh Circuit reversed the district court's decision to remand the claim under section 15(a), explaining that the *Bryant* holding was "quite limited."[149] Its decision regarding federal standing for Bryant's section 15(a) claim had even been accompanied by a warning: "We cautioned that our analysis was confined to the narrow violation the plaintiff alleged; we did not address standing requirements for claims under other parts of section 15(a)."[150]

As noted in the above synopsis of the *Bryant* case, Bryant's complaint cited only the first half of section 15(a), which states that the "private entity in possession of biometric identifiers or biometric information must develop a written policy, *made available to the public*, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information."[151] In contrast, Fox's complaint also included an allegation that the employer had failed to comply with the second half of section 15(a), which states that "a private entity in possession of biometric identifiers or biometric information *must comply with* . . . retention schedule and destruction guidelines."[152] Because Fox alleged that her former employer was wrongfully retaining her biometric information, the section 15(a) violation was not "a mere procedural failure to publicly disclose a data-retention policy" but rather an "invasion of a legally protected right."[153] The resulting injury, "though intangible, is personal and real, not general and abstract."[154]

In distinguishing the *Fox* decision from an earlier Seventh Circuit decision regarding the protection of personal information such as home address and phone number, the court emphasized the particularly sensitive nature of biometric information.[155] By enacting BIPA, the Illinois legislature intended to create robust protections for biometric identifiers "because they are immutable, and once compromised, are compromised forever."[156]

---

147. *Id.* at 1149.
148. *Id.* at 1150-51.
149. *Id.* at 1148-49.
150. *Id.*
151. 740 ILL. COMP. STAT. 14/15(a) (2021) (emphasis added).
152. *Id.* (emphasis added).
153. *Fox*, 980 F.3d at 1149.
154. *Id.*
155. *Id.* at 1155.
156. *Id.*

C. *THORNLEY V. CLEARVIEW AI, INC.*

Informed by the Seventh Circuit's decisions in *Bryant* and *Fox*, a plaintiff might succeed in stating a BIPA claim that satisfies the standing requirements in Illinois state court but falls short of the standing requirements for federal court, thereby ensuring that a lawsuit filed in state court remains in state court. For example, in *Thornley v. Clearview AI, Inc.*, the plaintiffs had filed a putative class action in Illinois state court, alleging that Clearview had secretly performed facial scans on photographs posted to the internet in order to create a facial recognition database, and then profited from the sale of that biometric data.[157] However, the plaintiffs did not base the complaint on BIPA section 15(b), which requires written consent to the collection of biometric information; instead, the plaintiffs brought only one claim against the defendant: a violation of BIPA section 15(c), which prohibits private companies from selling biometric information.[158] Further, the plaintiffs specified that "no class member, 'suffered any injury as a result of the violations of Section 15(c) of BIPA other than . . . statutory aggrievement.'"[159]

After Clearview removed the case to federal court, the plaintiffs argued that they lacked standing to proceed in federal court while Clearview countered that the plaintiffs did have standing.[160] The federal district court sided with the plaintiffs and remanded the case to state court.[161] On appeal, the Seventh Circuit affirmed the district court's decision to remand *Thornley* to state court.[162] After laying out the facts and procedural history of the case, the court listed the requirements for federal standing and explained that its analysis here would focus exclusively on the requirement that the plaintiff demonstrate "an injury in fact that is concrete, particularized, and actual or imminent."[163]

The court next revisited its previous rulings on BIPA cases, including *Bryant*[164] and *Fox*,[165] both discussed above. The court highlighted the fact that Bryant's claim under section 15(a) was *not* sufficient to establish federal standing because she alleged only a violation of a duty that was owed to the public; in contrast, Fox's claim under section 15(a) *was* sufficient to establish federal standing because she alleged an injury particular to her-

157. Thornley v. Clearview AI, Inc., 984 F.3d 1241, 1246 (7th Cir. 2021).
158. *Id.* at 1246.
159. *Id.* (quoting the complaint).
160. *Id.* at 1242.
161. *Id.*
162. *Thornley*, 984 F.3d at 1242.
163. *Id.* at 1244.
164. Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020).
165. Fox v. Dakkota Integrated Sys., LLC, 980 F.3d 1146 (7th Cir. 2020).

self.[166] To further clarify the reasons for the opposite outcomes for the two claims under section 15(a), the court went on to state that "allegations matter. One plaintiff may fail to allege a particularized harm to himself, while another may assert one . . . . [T]he result of the standing inquiry for the identical section of a statute will depend on what that section provides and what the plaintiff has alleged."[167]

Clearview, the defendant in this case, had removed the case from state court to federal court, and had then appealed the district court's decision to remand the case to state court; therefore, Clearview carried the burden of convincing the Seventh Circuit court that the plaintiffs had alleged an injury sufficient to establish federal standing.[168] With the aim of keeping the case in federal court, Clearview urged the Seventh Circuit to view its sale of biometric information as an injury-in-fact.[169] In reply, the court observed that the sale of information may well constitute an injury-in-fact in a different complaint, where the plaintiff asserted some sort of harm.[170]

After listing several examples of injuries that could plausibly be linked to the sale of biometric data, the court concluded that "[w]ithout any such allegations of concrete and particularized harm to the plaintiffs, we are left with a general rule that prohibits the operation of a market in biometric identifiers and information."[171] The court analogized this general rule to the Eagle Protection Act's regulatory prohibition against buying and selling eagles, eagle parts, eagle nests, or eagle eggs.[172] With that analogy in mind, a section 15(c) violation only implicates a general duty similar to a company's duty to make its schedule for retention and destruction of biometric information available to the public—unless the plaintiff alleges a particularized injury caused by the sale of the data.[173]

Is it as simple as that? Can plaintiffs keep a putative class action out of federal court merely by stating that the class they seek to represent *only* includes people who have not suffered an injury from the statutory violation? The answer seems to be yes. The Seventh Circuit raised the question of whether a district court might choose to take a broader view when the proposed class is purposely narrowed in such a way, but stated that it had "no reason to believe that the district court, acting on its own initiative,

166. *Thornley*, 984 F.3d at 1245.
167. *Id.* at 1246.
168. *Id.* at 1243-44.
169. *Id.* at 1247.
170. *Id.*
171. *Thornley*, 984 F.3d at 1247.
172. *Id.*
173. *Id.*

would certify a different and broader class; to that extent, the rule that the plaintiff controls her own case applies."[174]

And importantly, people who were excluded from this narrowly defined class would be free to sue Clearview if they wished to, either alone or as a member of a class alleging an injury.[175] Therefore, the restriction imposed on this class would not implicate *Standard Fire Insurance Co. v. Knowles*, where the Supreme Court held that a plaintiff could not keep a proposed class action in state court by stipulating that the class would not seek damages in excess of $5 million, because "a plaintiff who files a proposed class action cannot legally bind members of the proposed class before the class is certified."[176] When the restriction on the proposed class does not affect the legal rights of the members of the class, as in *Thornley*, there is "nothing [to] prevent a putative class representative from taking a conservative approach to class definition."[177]

In closing, the court noted that "[i]t is no secret to anyone that [the plaintiffs] took care in their allegations, and especially in the scope of the proposed class they would like to represent, to steer clear of federal court. But in general, plaintiffs may do this."[178] And though it observed that Illinois state courts permit BIPA complaints "that allege bare statutory violations, without any further need to allege or show injury,"[179] the Seventh Circuit expressed "no opinion on the adequacy of Thornley's complaint as a matter of Illinois law. That will be for the state court to address."[180]

In a concurring opinion, Circuit Judge Hamilton emphasized the point that the court's conclusion hinged on the fact that the *Thornley* plaintiffs tailored their claims and their description of the proposed class in very particular ways, and that "other plaintiffs might well establish [Article III] standing for other alleged violations of Section 15(c)"[181]—just as the court found Article III standing for a section 15(a) claim in *Fox*, but not in *Bryant*.

Next, the concurrence turned to an apparent inconsistency in recent decisions by the Seventh Circuit.[182] While the court had found federal standing for plaintiffs alleging intangible harm caused by violations of BIPA, the court had come to the opposite conclusion in recent decisions

174. *Id.* at 1247-48.
175. *Id.* at 1248.
176. *Thornley*, 984 F.3d at 1248 (quoting Standard Fire Ins. Co. v. Knowles, 568 U.S. 588, 593 (2013)).
177. *Id.*
178. *Id.*
179. *Id.* at 1248-49 (citing Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1203-04 (Ill. 2019)).
180. *Id.* at 1249.
181. *Thornley*, 984 F.3d at 1249 (Hamilton, J., concurring).
182. *Id.* at 1249-50.

related to other consumer-protection statutes, such as the Fair Credit Reporting Act and the Fair Debt Collection Practices Act.[183] After listing a number of cases on each side, Judge Hamilton wrote, "I confess that I have not yet been able to extract from these different lines of cases a consistently predictable rule or standard."[184]

In the *Spokeo* case (also discussed in the Seventh Circuit's *Bryant* and *Fox* decisions), the Supreme Court held that, although an intangible injury could satisfy the Article III requirement for a "concrete" injury, a "bare procedural violation" could not.[185] Noting that numerous federal courts subsequently concluded that plaintiffs had alleged only bare procedural violations, Judge Hamilton highlighted the fact that the Supreme Court itself had offered only one example of what might constitute a bare procedural violation—one which appears to be "utterly trivial": listing the wrong zip code for a debtor, in violation of the Fair Credit Reporting Act.[186]

In Judge Hamilton's view, the Seventh Circuit had taken *Spokeo* too far in several recent opinions, considering the Supreme Court's own reference point.[187] While lower federal courts had "spilled a great deal of ink" over what might, or might not, constitute a bare procedural violation,[188] Judge Hamilton turned instead to the discussion in *Spokeo* of the power of Congress to grant rights and define injuries that would provide a basis for alleging a concrete harm.[189]

Rather than focusing single-mindedly on the idea of a "bare procedural allegation," courts should give more "weight to *Spokeo*'s endorsement of standing where Congress has chosen to provide procedural and informational rights to reduce the risk of more substantive harm for consumers . . . and has created private rights of action to enforce them."[190] To show the implications of concluding too quickly that *Spokeo* would deny standing to a plaintiff, Judge Hamilton pointed to the potential creation of a "federal cousin" to BIPA.[191] If Congress were to provide for a private right of action to address violations of the law, courts might undermine the legislation by denying the existence of a concrete injury.[192] By extension, the courts would be undermining "legislative discretion to enforce federal law through private rights of action. The obvious alternative path for Congress [would]

183. *Id.* at 1250.
184. *Id.*
185. *Id.* (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).
186. *Thornley*, 984 F.3d at 1250 (Hamilton, J., concurring).
187. *Id.* at 1251.
188. *Id.* at 1250.
189. *Id.* at 1251.
190. *Id.*
191. *Thornley*, 984 F.3d at 1251 (Hamilton, J., concurring).
192. *Id.*

be to rely more heavily on enforcement through federal bureaucracies, which [would] face no standing obstacles."[193] In closing, Judge Hamilton expressed his hope for the Supreme Court to "revisit the problem of standing in private actions based on intangible injuries under a host of federal consumer-protection statutes."[194]

VI. CONCLUSION

In the years to come, advancements in technology are sure to broaden both the possibilities for utilizing biometric information and the concerns around biometric privacy. And while there is currently no federal law regulating biometric information,[195] a number of states have joined Illinois in implementing legislation to protect biometric privacy, including Texas, Washington, California, and New York.[196] Because BIPA is considered "the leading statute for biometric litigation," a number of states have looked to BIPA as a model as they draft their own biometric privacy legislation, with lawmakers in Maryland and South Carolina proposing bills with a private right of action.[197] In contrast, the law in Texas can only be enforced through the state's attorney general.[198]

The National Biometric Information Privacy Act of 2020 was introduced in Congress in August of that year; however, the bill died without receiving a vote.[199] As the name suggests, the bill was closely modeled on BIPA.[200] Like BIPA, the national law would have applied only to private entities and would have been enforced through a private right of action, with damages of $1,000 per negligent violation and $5,000 per intentional or reckless violation.[201]

---

193. *Id.*

194. *Id.*

195. Alicia Baiardo & Anthony Le, *U.S. Biometrics Laws Part I: An Overview of 2020*, JD SUPRA (Feb. 1, 2021), https://www.jdsupra.com/legalnews/u-s-biometrics-laws-part-i-an-overview-2275684/ [https://perma.cc/GLZ2-4CSU].

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

197. Baiardo & Le, *supra* note 195.

198. *Id.*

199. GOVTRACK, https://www.govtrack.us/congress/bills/116/s4400 [https://perma.cc/RW8S-VBN7].

200. Joseph J. Lazzarotti, *National Biometric Information Privacy Act, Proposed by Sens. Jeff Merkley and Bernie Sanders*, NAT'L L. REV. (Aug. 5, 2020), https://www.natlawreview.com/article/national-biometric-information-privacy-act-proposed-sens-jeff-merkley-and-bernie [https://perma.cc/DC87-CZ27].

201. National Information Privacy Act of 2020, S. 4400, 116th Cong., § 4(e)(1) (2020).

In the future, lawmakers in other states and in Congress will likely continue to look to BIPA as they decide whether to enforce biometric privacy legislation through a private right of action. Those lawmakers may be both cautioned and encouraged by the Seventh Circuit holdings regarding Article III standing in *Bryant*, *Fox*, and *Thornley*.