HOW TO RIDE THE LITIGATION ROLLERCOASTER DRIVEN BY THE BIOMETRIC INFORMATION PRIVACY ACT

Charles N. Insler*

The Biometric Information Privacy Act (BIPA)[1] is not just for Google and Facebook. While the technology giants have been sued for allegedly violating BIPA,[2] so too have countless other companies. In the last few years, plaintiffs have sued more than 200 companies across a range of industries (from locker rental companies to tanning salons) for allegedly violating BIPA.[3] Although BIPA is not a new statute, having been enacted in 2008, its application remains relatively recent. In December 2015, the U.S. District Court for the Northern District of Illinois noted that it was "unaware of any judicial interpretation of the statute."[4] So what is BIPA and why is it suddenly being invoked with such frequency?

BIPA IS THE FIRST, AND ARGUABLY MOST STRINGENT, BIOMETRIC STATUTE

The Illinois Legislature passed BIPA in October 2008 in the wake of Pay By Touch's bankruptcy.[5] At the time, Pay By Touch was operating the largest fingerprint scan system in Illinois, with its pilot system in use in a number of grocery stores, gas stations, and school cafeterias.[6] Pay By Touch's bankruptcy left thousands of individuals wondering what would become of their biometric data.[7] Biometric data—a person's unique

---

* Charles N. Insler is a partner in the St. Louis office of HeplerBroom LLC, where he concentrates on complex commercial litigation matters. He can be reached at *charles.insler@heplerbroom.com*. Versions of this article previously appeared in the *Illinois Bar Journal*, Vol. 106 #3, March 2018 and *The Computer & Internet Lawyer*, Vol. 35 #12, December 2018.

1 740 ILL. COMP. STAT. 14/1 (2008).

2 Rivera v. Google Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017); Gullen v. Facebook.com, Inc., No. 15-cv-7681, 2016 WL 245910 (N.D. Ill. Jan. 21, 2016).

3 *See, e.g.*, McCollough v. Smarte Carte, Inc., No. 16-cv-3777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016); Glynn v. eDriving, LLC, No. 2018 CH 7116 (Ill. Cir. Ct. June 5, 2018); Sekura v. Krishna Schaumberg Tan, Inc., No. 2016 CH 4945, 2017 WL 1181420 (Ill. Cir. Ct. Feb. 9, 2017) *rev'd and remanded*, 2018 IL App (1st) 180175; *see also* Becky Yerak, *Mariano's, Kimpton Hotels Sued Over Alleged Collection of Biometric Data*: *'It's Something Very Personal'*, CHI. TRIB. (July 21, 2017), https://www.chicagotribune.com/business/ct-employers-biometrics-lawsuits-0723-biz-20170720-story.html.

4 Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

5 *See Rivera*, 238 F. Supp. 3d at 1098.

6 740 ILL. COMP. STAT. 14/5(b) (2008).

7 *Rivera*, 238 F. Supp. 3d at 1098.

biological traits embodied in a fingerprint, voice print, retinal scan, or facial geometry—is the most sensitive data belonging to an individual. Unlike a PIN code or a social security number, once biometric data is compromised, "the individual has no recourse, is at [a] heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[8] BIPA establishes safeguards and procedures relating to the retention, collection, disclosure, and destruction of biometric data in light of these concerns.[9]

BIPA defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," and "biometric information" as information based on "biometric identifiers."[10] Writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color are excluded from these definitions.[11] On the retention and destruction front, BIPA requires that a private entity (the statute does not apply to the state or government agencies):

> [D]evelop 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.[12]

Before collecting biometric data, a private entity must inform the individual that a biometric identifier, or biometric information, is being collected and inform them of the purpose and length of the collection and storage of their biometric information.[13] These disclosures must be in writing and the individual must provide a written release.[14] Private entities may not sell biometric identifiers and biometric information to third parties and must treat biometric data as sensitive and confidential and store, transmit, and protect the information "using the reasonable standard of care within the private entity's industry."[15] Individuals that prevail in a BIPA action "may recover the greater of $1,000 in liquidated damages, or actual damages, for each negligent violation of the statute, and the greater of $5,000 in liquidated damages, or actual damages, for each reckless or intentional violation of the

---

8 740 ILL. COMP. STAT. 14/5(c) (2008).
9 *Id.* § 14/15.
10 *Id.* § 14/10.
11 *Id.*
12 *Id.* § 14/15(a).
13 *Id.* § 14/15.
14 *Id.* § 14/15(b).
15 *Id.* § 14/15(c), (e).

statute.[16] Attorneys' fees and injunctive relief are also available to a prevailing party.[17]

Illinois is not alone in expressing concern over the use of biometric data. Washington and Texas have also passed biometric privacy laws.[18] But unlike BIPA, neither Washington nor Texas allows for a private cause of action; enforcement under these statutes is left to the state Attorney General.[19] Lawmakers in Alaska, Montana, and New Hampshire have proposed biometric laws that would allow private causes of action, but those bills have stalled, leaving Illinois as the only state that currently authorizes private citizens to sue for the alleged misuse of their biometric data *before* any unauthorized access or data breach.[20] California's recently passed Consumer Privacy Act of 2018 (which takes effect on January 1, 2020) does not change this. The Consumer Privacy Act includes biometric information within its protections of "Personal Information," but the Consumer Privacy Act's private right of action relates to the "unauthorized access and exfiltration, theft, or disclosure" of the consumer's personal information.[21]

BIPA LAWSUITS ARE LARGELY ABOUT PUNCH CLOCKS

With talk of voiceprints and retina scans, BIPA may conjure up scenes from futuristic films like *Blade Runner* or *Minority Report*. To be sure, some of the technology involved in BIPA lawsuits is cutting-edge, touching on facial-recognition software for photographs[22] and storage lockers operated by fingerprints.[23] But most of the lawsuits concern a far more quotidian technology: the punch clock. Updated for the digital era, punch clocks have gone from stamping a punch card to scanning an employee's fingerprint.[24] With the technology available for a few hundred dollars, many employers

---

16 *Id.* § 14/20.

17 *Id.*

18 2017 Wash. Sess. Laws 299 (S.H.B. 1493); TEX. BUS. & COM. CODE ANN. §503.001 (West 2018).

19 Paul Shukovksy, *Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin*, BLOOMBERG (July 18, 2017), https://www.bna.com/washington-biometric-privacy-n73014461920/ (The Washington statute also provides that consent is "context-dependent," eschewing BIPA's requirement of informed written consent.).

20 *See* H.B. 72, 30th Leg., Reg. Sess. (Alaska 2017); H.B. 518, 65th Leg., Reg. Sess. (Mont. 2017); H.B. 523, Reg. Session (N.H. 2017). Several states include biometric information within their general protections for data breaches, but those statutes regulate biometric data only after there has been unauthorized access. BIPA regulates the collection and retention of biometric data *before* there is any data breach or unauthorized access. *See* 740 ILL. COMP. STAT. 14/1 (2008).

21 CAL. CIV. CODE § 1798.150(a)(1) (2018).

22 Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1095 (N.D. Ill. 2017); Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

23 McCollough v. Smarte Carte, Inc., No. 16-cv-3777, 2016 WL 4077108, at *1 (N.D. Ill. Aug. 1, 2016).

24 Yerak, *supra* note 3.

have begun shifting to these biometric timekeeping devices, which can keep more accurate hours and eliminate the risk of "buddy punching."[25]

This, in turn, has exposed employers to BIPA lawsuits—and in droves.[26] Employers who use fingerprint scans are highly susceptible to a BIPA lawsuit, as demonstrated by recent filings and by Internet advertisements and websites promising those who have "been fingerprinted for a job" that they "could be owed money."[27] In almost all cases, the plaintiffs bring these lawsuits as class actions, on behalf of all similarly situated employees.[28] Their status as class actions has the potential to amplify damages dramatically, with one BIPA class action lawsuit settling for $1.5 million.[29] Their status as class actions may also make the cases removable to federal court under the Class Action Fairness Act.[30]

DEFENDANTS ARE FIGHTING BIPA LAWSUITS UNDER DIFFERENT THEORIES, WITH VARYING SUCCESS

Illinois statutes do not have extraterritorial effect unless the General Assembly expressly intends such an effect.[31] BIPA is one such statute that does not apply beyond Illinois's borders.[32] In the digital world, where the alleged conduct at issue may occur in the cloud or on remote servers, BIPA may have no application.[33] Google made this argument in *Rivera*, but to no avail; the District Court denied Google's motion to dismiss, noting that the photographs that were subject to facial recognition software were taken in Illinois, by Illinois residents, and uploaded to the Google-Photos cloud-based

---

25 *Id.* As an aside, the U.S. Court of Appeals for the Fourth Circuit has held that an employer was liable for failing to accommodate an employee's religious objections to using a digital scanner. EEOC v. Consol. Energy, Inc., 860 F.3d 131, 143 (4th Cir. 2017).

26 *See, e.g.*, Grabowska v. Millard Maint. Co., No. 2017-CH-13730, 2017 WL 4767159 (Ill. Cir. Ct. Oct. 12, 2017) (Complaint at ¶ 2) ("Millard employees in Illinois have been required to clock 'in' and 'out' of their work shifts by scanning their fingerprints, and Millard's biometric computer systems then verify the employee . . . ."); Henderson v. Signature Healthcare Servs., LLC, No. 2017-CH-12686, 2017 WL 4316165 (Ill. Cir. Ct. Sept. 19, 2017) (Complaint at ¶2) ("When employees first begin their jobs at Chicago Lakeshore Hospital, they are required to scan their fingerprint in its time clock. That's because [the hospital] uses a biometric time tracking system . . . instead of key fobs or identification cards.").

27 *Have You Been Fingerprinted for a Job? Know Your Rights and Fight Back!*, CLASS ACTION FINDER, http://classactionfinder.com/fingerprint/ (last visited Mar. 1, 2019).

28 *See, e.g.*, Warren v. Meijer, Inc., No. 2017-CH-13723, 2017 WL 4767156 (Ill. Cir. Ct. Oct. 12, 2017) (Complaint at ¶ 49).

29 Yerak, *supra* note 23.

30 Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 502 (S.D.N.Y. 2017), *aff'd in part, vacated in part, remanded sub nom.* Santana v. Take-Two Interactive Software, Inc., No. 17-303, 2017 WL 5592589 (2d Cir. Nov. 21, 2017) (Summary Order).

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

32 *Id.*; Monroy v. Shutterfly, Inc., No. 16-CV-10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017).

33 *Rivera*, 238 F. Supp. 3d at 1100.

service from an Illinois IP address.[34] At the same time, the court noted that the issue was a "complex" one and that neither side had "addressed it thoroughly."[35]

Challenges under the Constitution's Dormant Commerce Clause have dovetailed with the extraterritorial arguments. A challenge under the Dormant Commerce Clause argues that the application of one state's law would have the practical effect of controlling conduct beyond the boundaries of that state.[36] In other words, enforcing BIPA in Illinois would effectively enforce BIPA in California (and other states), even though the other state may have rejected similar legislation.[37] The District Court rejected this argument in *Monroy*, stating that Alejandro Monroy's lawsuit was limited to individuals whose biometric data was obtained from photographs uploaded to Shutterfly in Illinois.[38]

Many of the large technology companies are headquartered in California and incorporated in Delaware, raising issues of personal jurisdiction. In *Norberg*, Shutterfly moved for dismissal under Rule 12(b)(2).[39] The District Court denied the motion, noting that Shutterfly offered its photo sharing and printing services to Illinois citizens, shipped its products directly to Illinois, and was accused of violating an Illinois statute arising out of its Illinois contacts.[40] Facebook, on the other hand, won dismissal of its BIPA case on Rule 12(b)(2) grounds, with the District Court holding that simply operating a Web site accessible to Illinois residents did not confer specific jurisdiction particularly where no allegation was present that "Facebook targets its alleged biometric collection activities at Illinois residents . . . ."[41] Facebook has since been defending this lawsuit in California federal court (see below).[42]

Article III standing arguments are featured prominently in BIPA litigation.[43] Under the U.S. Supreme Court's recent decision in *Spokeo Inc.*

---

34 *Id.* at 1102.

35 *Id.*; *see also Monroy*, 2017 WL 4099846, at *6 (noting that Shutterfly could raise the issue at a later time when the record was clearer).

36 *See Monroy*, 2017 WL 4099846, at *7.

37 *See id.* at *5.

38 *Id.* at *7; *see also Rivera*, 238 F. Supp. 3d at 1104 (noting that this argument required a better factual understanding of what was happening in the Google Photos face-scan process).

39 Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).

40 *Id.* at 1106.

41 Gullen v. Facebook.com, Inc., No. 15-CV-7681, 2016 WL 245910, *2 (N.D. Ill. Jan. 21, 2016).

42 *See* Gullen v. Facebook, Inc., No. 3:16-CV-00937-JD, 2018 WL 1989497, (N.D. Cal. Mar. 2, 2018).

43 Miller v. Southwest Airlines Co., No. 18 C 86, 2018 WL 4030590, at *3 (N.D. Ill. Aug. 23, 2018); Aguilar v. Rexnord LLC, No. 17 CV 9019, 2018 WL 3239715, at *4 (N.D. Ill. July 3, 2018); Howe v. Speedway LLC, No. 17-CV-07303, 2018 WL 2445541, at *7, *7 n.5 (N.D. Ill. May 31, 2018); Dixon v. Washington & Jane Smith Cmty., No. 17 C 8033, 2018 WL 2445292, at *11-12 (N.D. Ill. May 31, 2018); McCollough v. Smarte Carte, Inc., No. 16-CV-3777, 2016 WL 4077108, at *3-5 (N.D. Ill. Aug. 1, 2016).

v. Robins,[44] Article III standing requires a plaintiff to allege an injury-in-fact that is both concrete and particularized.[45] In *McCollough*, the District Court found that the plaintiff had failed to adequately allege a concrete injury from the use of her fingerprints to open and close Smarte Carte's locker, even though Smarte Carte had committed a "technical violation" of BIPA by failing to obtain the plaintiff's advance notice and failing to inform the plaintiff of the company's retention policy.[46] Holding that McCollough "undoubtedly understood when she first used the system that her fingerprint data would have to be retained until she retrieved her belongings from the locker," the court concluded that McCollough could not demonstrate any actual injury as required by Article III.[47] The *McCollough* court went a step further and also held McCollough was not an "aggrieved" person within the meaning of the statute.[48] Other cases from the Northern District of Illinois have reached the opposite conclusions, holding a plaintiff's complaint adequately alleged Article III standing.[49] On the whole though, the "vast majority of [federal] courts to have evaluated standing in this context have acknowledged that more than 'bare procedural violations' of the statute must be alleged to satisfy the requirement of a 'concrete and particularized' injury that is 'actual or imminent, not conjectural or hypothetical' under *Spokeo*."[50]

These holdings are now in serious doubt. On January 25, 2019, the Illinois Supreme Court resolved the existing split in authority on how best to interpret the meaning of the word "aggrieved" by holding a person is aggrieved in the legal sense "when a legal right is invaded by the act complained of . . . ."[51] In other words, a "violation [of the statute], *in itself*, is sufficient to support the individual's or customer's statutory cause of

---

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

45 *McCollough*, 2016 WL 4077108 at *3.

46 *Id.*

47 *Id.* at *4; *see also* Vigil v. Take-Two Interactive Software, Inc., 235 F. Supp. 3d 499, 519 (S.D.N.Y. 2017) ("The plaintiffs cannot aggregate multiple bare procedural violations to create [Article III] standing where no injury-in-fact otherwise exists.").

48 *McCollough*, 2016 WL 4077108 at *3; *Vigil*, 235 F. Supp. 3d at 519-20 (following *McCollough*).

49 *See, e.g.*, Dixon v. Washington & Jane Smith Cmty., No. 17 C 8033, 2018 WL 2445292, at *12 (N.D. Ill. May 31, 2018) (finding the plaintiff had alleged "an actual and concrete injury to her right to privacy in her biometric data stemming from the defendants' alleged BIPA violations" and concluding that plaintiff was a "'person aggrieved' with a right of action under the statute"). *But see* Aguilar v. Rexnord LLC, No. 17 CV 9019, 2018 WL 3239715, at *4 (N.D. Ill. July 3, 2018); (holding that the statutory violations of privacy and emotional injuries pleaded in the complaint did not constitute injuries in fact); Howe v. Speedway LLC, No. 17-CV-07303, 2018 WL 2445541, at *7, *7 n.5 (N.D. Ill. May 31, 2018) (finding defendants' procedural violations did not cause plaintiff an injury-in-fact, but declining to express an opinion as to whether plaintiff qualified as a "'person aggrieved'" by the statute).

50 Goings v. UGN, Inc., No. 17-CV-9340, 2018 WL 2966970, at *2 (N.D. Ill. June 13, 2018) (collecting cases).

51 Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 30.

action."[52] No additional injury or damages are required.[53] Even a "technical" violation of the statute produces a "real and significant" injury.[54]

The underlying goals of BIPA support this result.[55] If the purpose of BIPA was to safeguard biometric identifiers and information *before* the data was compromised, then individuals must be permitted to enforce those protective rights as soon as they became aware of a defendant's failure to properly protect their biometric data.[56] To hold otherwise and require "individuals to wait until they have sustained some compensable injury beyond violation of their statutory rights . . . would be completely antithetical to the Act's preventative and deterrent purposes."[57]

The Illinois Supreme Court's *Rosenbach* decision was presaged by the *Facebook* decision from the U.S. District Court for the Northern District of California, in which that Court noted the appellate decision in *Rosenbach* was not a good predictor "of how the Illinois Supreme Court would interpret 'aggrieved' under BIPA."[58] Relying on other decisions from the Illinois Supreme Court, the *Facebook* court certified "a class of Facebook users located in Illinois for whom Facebook created and stored a face template after June 7, 2011."[59] The *Facebook* decision is currently on appeal to the U.S. Court of Appeals for the Ninth Circuit.[60]

Finally, Google and others have argued that their technology did not fall within BIPA's definition of biometric identifier or biometric information. These arguments have not been successful at the dismissal stage.[61]

CONCLUSION

The Supreme Court's ruling in *Rosenbach v. Six Flags* is likely to further embolden lawsuits asserting bare violations of the statute and have an immediate impact on businesses in Illinois.[62] The effect of the law is already

---

52 *Id.* ¶ 33 (emphasis added).

53 *See id.*

54 *Id.* ¶ 34.

55 *Id.* ¶¶ 24-37.

56 *See id.* ¶ 37.

57 *Id.*

58 *In re* Facebook Biometric Info. Privacy Litig., No. 3:15-CV-03747-JD, 2018 WL 1794295, at *6-8 (N.D. Cal. Apr. 16, 2018).

59 *Id.* at *10.

60 Patel v. Facebook, Inc., 290 F. Supp. 3d 948 (N.D. Cal. 2018), *appeal docketed*, No. 18-15982 (9th Cir. May 30, 2018).

61 Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017) (denying motion to dismiss based on Google's argument that a scan of facial geometry from a photograph was not a biometric identifier); Monroy v. Shutterfly, Inc., No. 16-cv-10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017) (denying motion to dismiss based on Google's argument that a scan of facial geometry from a photograph was not a biometric identifier).

62 The next source of litigation surrounding BIPA may center on whether defendants have insurance coverage for these disputes. On August 30, 2018, Zurich American Insurance Company and

being seen beyond the courtroom. BIPA is believed to be behind Nest's decision not to offer facial recognition on doorbells operating in Illinois and Google's decision not to allow Illinois users to match their selfies with faces depicted in works of art.[63] Companies in Illinois may want to hold on: after the *Six Flags* decision they could be in for a wild ride.

American Guarantee & Liability Company filed suit against their insured, Omnicell, Inc., seeking a declaration that there was no coverage for an underlying BIPA lawsuit against Omnicell. *See* Zurich Am. Ins. Co. v. Omnicell, Inc., No. 5:18-CV-5345-NC (N.D. Cal. Aug. 30, 2018).

63 Ally Marotti, *Illinois Supreme Court Rules Against Six Flags in Lawsuit Over Fingerprint Scans. Here's Why Facebook and Google Care.*, CHI. TRIB. (Jan. 25, 2019), http://chicagotribune.com/business/ct-biz-biometrics-lawsuit-20190125-story.html.