The Computer & Internet Lawyer

Volume 35 ▲ Number 12 ▲ DECEMBER 2018

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

How to Tackle Litigation under the Biometric Information Privacy Act

By Charles N. Insler

The Biometric Information Privacy Act (BIPA), a 10-year-old Illinois state law,[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 months, plaintiffs have sued dozens of 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 US 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 applied with such frequency?

BIPA Is the First, and Arguably Most Stringent, Biometrics 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 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):

> … develop a written policy, made available to the public, establishing a retention schedule and

Charles N. Insler is an attorney with Hepler Broom in St. Louis, Missouri, where he concentrates on complex commercial litigation matters. He can be reached at *charles.insler@heplerbroom.com*. This article is reprinted with permission from the *Illinois Bar Journal*, Vol. 106 #3, March 2018.

> 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. These disclosures must be in writing and the individual must provide a written release.[13] 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.[14] 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 statute.[15] Attorneys' fees and injunctive relief are also available to a prevailing party.[16]

Illinois is not alone in expressing concern over the use of biometric data. Washington and Texas have also passed biometric privacy laws.[17] Unlike BIPA, neither Washington nor Texas allows for a private cause of action; enforcement under these statutes is left to the state Attorney General.[18] 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.[19] 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.[20]

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,[21] and storage lockers operated by fingerprints.[22] Many of the lawsuits concern a 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. With the technology available for a few hundred dollars, many employers have begun shifting to these biometric timekeeping devices, which can keep more accurate hours and eliminate the risk of "buddy punching."[23]

This, in turn, has exposed employers to BIPA lawsuits—and in droves.[24] Employers who use fingerprint scans are highly susceptible to a BIPA lawsuit, as demonstrated by recent filings and by Internet advertisements promising those who have "been fingerprinted for a job" that they "could be owed money." In almost all cases, the plaintiffs bring these lawsuits as class actions, on behalf of all similarly situated employees.[25] Their status as class actions has the potential to amplify damages dramatically, with one BIPA class action lawsuit settling for $1.5 million.[26] Their status as class actions may also make the cases removable to federal court under the Class Action Fairness Act.[27]

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.[28] BIPA is one such statute that does not apply beyond Illinois's borders.[29] In the digital world, where the alleged conduct at issue may occur in the cloud or on remote servers, BIPA may have no application.[30] 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 service from an Illinois IP address.[31] At the same time, the court noted that the issue was a "complex" one and that neither side had "addressed it thoroughly."[32]

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. 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.[33] The District Court rejected this argument in *Monroy*, stating that Alejandro Monroy's lawsuit was limited to individuals whose biometric data were obtained from photographs uploaded to Shutterfly in Illinois.[34]

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).[35] 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.[36] 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 there was no allegation that "Facebook targets its alleged biometric collection activities at Illinois residents …"[37] Facebook has since been defending this lawsuit in California federal court (see below).

Article III standing arguments have featured prominently in BIPA litigation.[38] Under the US Supreme Court's recent decision in *Spokeo Inc. v. Robins*,[39] Article III standing requires the plaintiff to allege an injury-in-fact that is both concrete and particularized.[40] In *McCullough*, 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.[41] 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.[42] The *McCollough* court went a step further and also held that McCollough was not an "aggrieved" person within the meaning of the statute.[43] Other cases from the Northern District of Illinois have come to the opposite conclusions, and held that a plaintiff's complaint adequately alleged Article III standing.[44] 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.*"[45]

The Illinois Appellate Court, Second District, has followed *McCollough's* reasoning.[46] In *Rosenbach,* the Second District accepted a certified question from the Circuit Court of Lake County to answer whether BIPA required "a person aggrieved by a violation of [the] Act" to allege an actual harm.[47] Reviewing *McCollough*, Black's Law Dictionary, and other authorities, the Second District held that if "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 in section 20."[48] The Second District did note, however, that an "injury or adverse effect need not be pecuniary."[49] The *Rosenbach* decision is currently on appeal to the Illinois Supreme Court.[50]

Rosenbach is not without its critics. In *Facebook*, the US District Court for the Northern District of California found that *Rosenbach* was not a good predictor "of how the Illinois Supreme Court would interpret 'aggrieved' under BIPA."[51] 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."[52] The *Facebook* decision is currently on appeal to the US Court of Appeals for the Ninth Circuit.[53] The Illinois Appellate Court, First District, recently joined *Facebook* in its approach to interpreting "aggrieved," splitting with the Second District's interpretation.[54]

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.[55]

Conclusion

The last few months have seen an explosion in litigation under BIPA.[56] With technology constantly evolving and advancing, particularly in the biometric field, BIPA will be a topic of discussion and a source of litigation for years to come. In short, BIPA will remain a part of our litigation landscape, a part of our dispute DNA.

Notes

1. 740 Ill. Comp. Stat. 14/1 et seq.
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., McCullough 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), *reversed and remanded,* 2018 IL App (1st) 180175; *see also* Becky Yerak, *Marioano's, Kimpton Hotels Sued Over Alleged Collection of Biometric Data,* Chicago Tribune (July 21, 2017).
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 ILCS 14/5(b).
7. *Rivera,* 238 F. Supp. 3d at 1098.

8. 740 ILCS 14/5(c).
9. 740 ILCS 14/15.
10. 740 ILCS 14/10.
11. *Id*.
12. 740 ILCS 14/15(a).
13. 740 ILCS 14/15(b).
14. 740 ILCS 14/15(c), (e).
15. 740 ILCS 14/20.
16. *Id*.
17. 2017 Wash. Legis. Serv. Ch. 299 (S.H.B. 1493); Tex. Bus. & Com. Code Ann. §503.001.
18. Paul Shukovksy, "Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin," *Bloomberg BNA* (July 18, 2017). The Washington statute also provides that consent is "context-dependent," eschewing BIPA's requirement of informed written consent. *See id*.
19. *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.
20. Cal. Civ. Code § 1798.150(a)(1) (2018).
21. *Rivera,* 238 F. Supp. 3d at 1095; *Norberg,* 152 F. Supp. 3d at 1106.
22. *McCullough,* 2016 WL 4077108, at *1.
23. Yerak, *Marioano's, Kimpton Hotels Sued Over Alleged Collection of Biometric Data*. As an aside, the US 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).
24. *See, e.g., Grabowska v. Millard Maintenance 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 Services, 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.").
25. *See, e.g., Warren v. Meijer, Inc.,* No. 2017-CH-13723, 2017 WL 4767156 (Ill. Cir. Ct. Oct. 12, 2017) (Complaint at ¶49).
26. Yerak, *Marioano's, Kimpton Hotels Sued Over Alleged Collection of Biometric Data*.
27. *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).
28. *Rivera,* 238 F. Supp. 3d at 1100.
29. *Id.; Monroy v. Shutterfly, Inc.,* No. 16-cv-10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017).
30. *Rivera,* 238 F. Supp. 3d at 1100.
31. *Id*. at 1102.
32. *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).
33. *See Monroy,* 2017 WL 4099846, at *5.
34. *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).
35. *Norberg,* 152 F. Supp. 3d at 1105.
36. *Id*.
37. *Gullen*, 2016 WL 245910, at *2.
38. *Miller v. Southwest Airlines,* 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.-Beverly*, No. 17 C 8033, 2018 WL 2445292, at *12 (N.D. Ill. May 31, 2018); *McCullough*, 2016 WL 4077108 at *3-*5.
39. 136 S. Ct. 1540 (2016).
40. *McCullough*, 2016 WL 4077108 at *3.
41. *Id*.
42. *Id*. at *4; *see also Vigil,* 235 F. Supp. 3d at 519 ("The plaintiffs cannot aggregate multiple bare procedural violations to create [Article III] standing where no injury-in-fact otherwise exists.").
43. *McCullough*, 2016 WL 4077108 at *3*; Vigil,* 235 F. Supp. 3d at 519-20 (following *McCollough*).
44. *See, e.g., Dixon,* 2018 WL 2445292, at *12 (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,* 2018 WL 3239715, at *4 (holding that the statutory violations of privacy and emotional injuries pleaded in the complaint did not constitute injuries in fact); *Howe*, 2018 WL 2445541, at *7, *7 n.5 (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).
45. *Goings v. UGN, Inc.*, No. 17-CV-9340, 2018 WL 2966970, at *2 (N.D. Ill. June 13, 2018) (collecting cases).
46. *Rosenbach v. Six Flags Entm't Corp.*, 2017 IL App (2d) 170317, ¶21.
47. *Id*. at ¶1.
48. *Id*. at ¶28.
49. *Id*.
50. *Rosenbach v. Six Flags Entm't Corp.,* No. 123186 (Ill.).
51. *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).

52. *Id*. at *10.
53. *Patel v. Facebook, Inc.,* No. 18-15982 (9th Cir. May 30, 2018).
54. *Sekura v. Krishna Schaumburg Tan, Inc.*, 2018 IL App (1st) 180175, at ¶74 ("The *Rosenbach* court found that it had to find that an additional harm was required; otherwise the word 'aggrieved' in the Act would be rendered superfluous … We already examined this argument … and found it unpersuasive.").
55. *Rivera,* 238 F. Supp. 3d at 1100 (denying motion to dismiss based on Google's argument that a scan of facial geometry from a photograph was not a biometric identifier); *Monroy,* 2017 WL 4099846, at *5 (same).
56. 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 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) (Doc. 1).