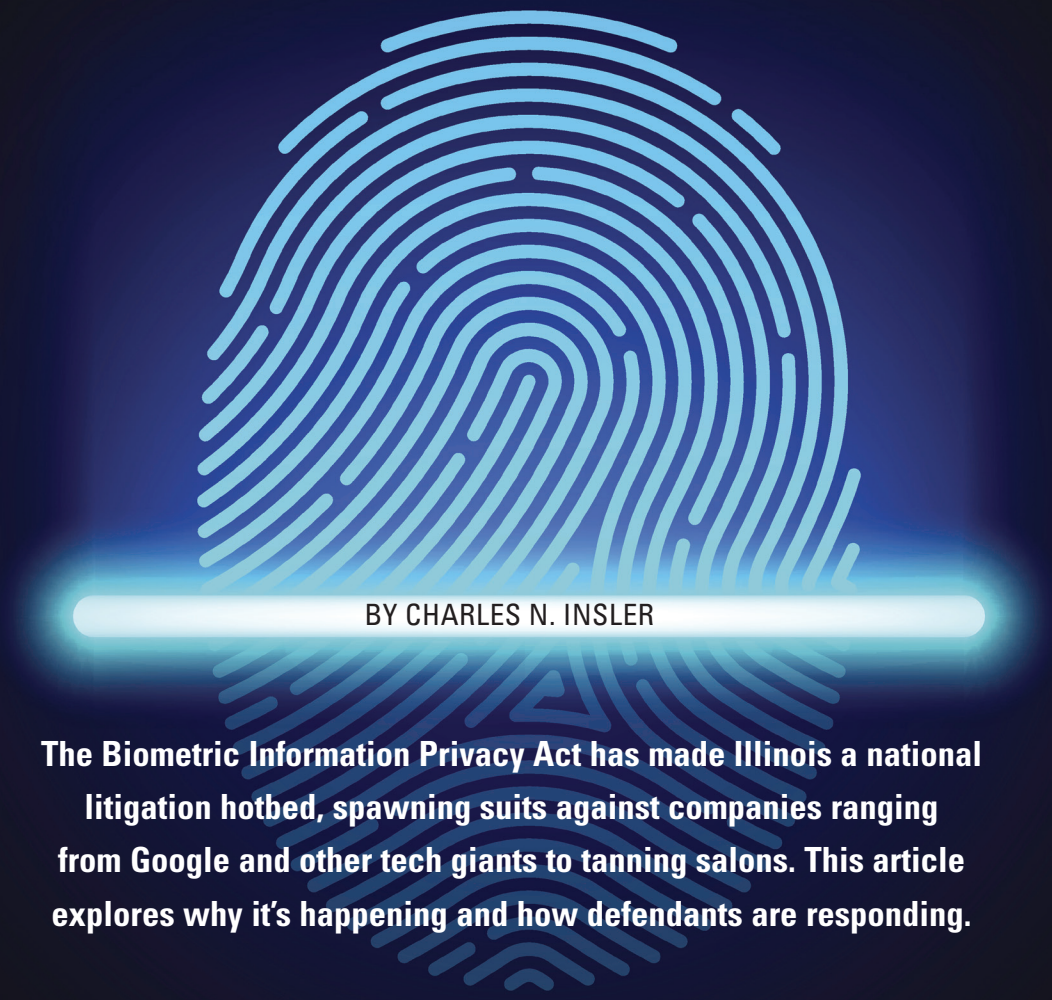
# Understanding the Biometric Information Privacy Act Litigation Explosion



BY CHARLES N. INSLER

**The Biometric Information Privacy Act has made Illinois a national litigation hotbed, spawning suits against companies ranging from Google and other tech giants to tanning salons. This article explores why it's happening and how defendants are responding.**

**CHARLES N. INSLER** *is an attorney with Hepler Broom in St. Louis, where he concentrates on complex commercial litigation matters.*

charles.insler@heplerbroom.com

**AS MULTIPLYING NEWS ACCOUNTS MAKE CLEAR, ILLINOIS' BIOMETRIC** Information Privacy Act ("BIPA")[1] is the basis for high-profile lawsuits against Google, Facebook, and other tech behemoths. But the litigation hasn't stopped there.

While the technology giants have been sued for allegedly violating BIPA,[2] so too have countless other companies. In recent months, plaintiffs have sued more than 30 companies across a range of industries, from locker rental companies to tanning salons, for allegedly violating BIPA.[3]

BIPA is not a new statute – it was enacted in 2008 – but its application is 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 applied with such frequency?

## BIPA: The first, and arguably most stringent, biometrics statute

The Illinois Legislature passed BIPA in October 2008 in the wake of the bankruptcy of Pay By Touch,[5] which was operating the largest fingerprint scan system in Illinois. Its pilot program was in use in a number of grocery stores, gas stations, and school cafeterias.

Pay By Touch's bankruptcy left thousands of individuals wondering what would become of their fingerprints, a form of biometric data. Biometric data – a person's unique biological traits embodied in not only fingerprints but also voice prints, retinal scans, 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."[6] BIPA establishes safeguards and procedures for the retention, collection, disclosure, and destruction of biometric data in light of these concerns.

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."[7] 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.[8] On the retention and destruction front, BIPA requires that a 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 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.[9]

Before collecting biometric data, a private entity must tell individuals 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.[10]

BIPA prohibits a private entity from

1. 740 ILCS 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); *Sekura v. Krishna Schaumberg Tan, Inc.*, No. 2016 CH 4945 (Ill. Cir. Ct. Feb. 9, 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(c).
7. *Id.* at § 14/10.
8. *Id.*
9. *Id.* at § 14/15(a).
10. *Id.* at § 14/15(b).

### TAKEAWAYS >>

- 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. In order to establish safeguards and procedures relating to the retention, collection, disclosure, and destruction of biometric data, Illinois enacted the Biometric Information Privacy Act ("BIPA") in 2008.

- Before collecting biometric data, BIPA requires a private entity to 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.

- The last few months have seen an explosion in litigation under BIPA. 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.

ILLINOIS IS THE ONLY STATE THAT AUTHORIZES PRIVATE CITIZENS TO SUE FOR THE ALLEGED MISUSE OF THEIR BIOMETRIC DATA.

disseminating biometric identifiers and biometric information without the individual's written consent, unless the disclosure is needed to complete a previously authorized financial transaction.[11] Private entities may not, therefore, sell biometric identifiers and biometric information to third-parties.[12] Instead, they 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."[13]

Illinois is not alone in regulating the use of biometric data. Washington and Texas have also passed biometric privacy laws.[14] But unlike BIPA, neither the Washington nor Texas law provides for a private cause of action; enforcement under these statutes is left to the state attorney general. 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.

"Any person aggrieved by a violation of [BIPA] shall have a right of action [in court]...against an offending party" and 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] Attorney fees and injunctive relief are also available to a prevailing party.[16]

## Punch-clock lawsuits

With its references to voiceprints and retina scans, BIPA may suggest scenes from *Blade Runner* or *Minority Report*. And to be sure, some of the technology involved in BIPA lawsuits is cutting-edge, touching on facial-recognition software for photographs and storage lockers operated by fingerprints.

But 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. And 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."

This, in turn, has exposed employers to BIPA lawsuits – more than 30 suits from July to October 2017.[17] 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. Their status as class actions has the potential to amplify damages dramatically, with one BIPA class action lawsuit settling for $1.5 million.[18] Class actions are also potentially removable to federal court under the Class Action Fairness Act.[19]

## Fighting BIPA lawsuits

Defendants have used various theories to challenge BIPA lawsuits. The results have been mixed.

**Extraterritoriality.** Illinois statutes do not have extraterritorial effect unless the General Assembly expressly intends such an effect, which means that BIPA does not apply beyond Illinois' borders. Consequently, it can be argued that in the digital world – where the alleged conduct may occur in the cloud or on remote

11. *Id.* at § 14/15(d).
12. *Id.* at § 14/15(c).
13. *Id.* at § 14/15(e).
14. 2017 Wash. Legis. Serv. Ch. 299 (S.H.B. 1493); Tex. Bus. & Com. Code Ann. § 503.001.
15. 740 ILCS 14/20.
16. *Id.*
17. 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.").
18. Becky Yerak, *Marioano's, Kimpton Hotels Sued Over Alleged Collection of Biometric Data*, Chicago Tribune (July 21, 2017).
19. *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).

**ISBA RESOURCES >>**

- Matthew Hector, *Illinois' Biometric Privacy Law Back in the News*, 105 Ill. B.J. 12 (Dec. 2017), https://www.isba.org/ibj/2017/12/lawpulse/illinoisbiometricprivacylawbacknews.
- Matthew Hector, *Court: Suit Based Solely on Technical Violations of Biometric Privacy Law Can't Go Forward*, 106 Ill. B.J. 2 (Feb. 2017), https://www.isba.org/ibj/2018/02/lawpulse/courtsuitbasedsolelyontechnicalviol.
- Matthew Hector, *Class Action Suit Alleges Google Is Violating Illinoisans' 'Biometric' Privacy*, 104 Ill. B.J. 5 (May 2016), https://www.isba.org/ibj/2016/05/lawpulse/classactionsuitallegesgoogleisviola.

servers – BIPA has no application.

Google made this argument in *Rivera v. Google, Inc.* but to no avail; the district court denied Google's motion to dismiss. The court observed that the photographs 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.[20] At the same time, the court noted that the issue was "complex" and that neither side had "addressed it thoroughly."[21]

**Dormant Commerce Clause.** Challenges under the U.S. Constitution's so-called Dormant Commerce Clause have dovetailed with the extraterritorial arguments. This theory posits that applying 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 California has rejected similar legislation. The district court rejected this argument in *Monroy v. Shutterfly, Inc.*, opining that Alejandro Monroy's lawsuit was limited to individuals whose biometric data was obtained from photographs uploaded to Shutterfly in Illinois.[22]

**Personal jurisdiction.** Many of the large technology companies are headquartered in California and incorporated in Delaware, raising issues of personal jurisdiction. In *Norberg v. Shutterfly, Inc.*, Shutterfly moved for dismissal under Rule 12(b)(2).[23] 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.

Facebook, on the other hand, won dismissal of its BIPA case on Rule 12(b)(2) grounds. The district court held that simply operating a website 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...."[24]

**Standing.** Article III standing arguments have featured prominently in BIPA litigation. Under the U.S. Supreme Court's recent decision in *Spokeo Inc. v. Robins*,[25] Article III standing requires the plaintiff to allege an injury-in-fact that is both concrete and particularized.

In *McCollough v. Smarte Carte, Inc.*, 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.[26] 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.[27] The *McCollough* court went a step further and also held that McCollough was not an "aggrieved" person within the meaning of the statute.[28]

The Illinois Appellate Court, Second District, has followed *McCollough's* reasoning in what appears to be the first appellate decision from Illinois to address BIPA.[29] In *Rosenbach v. Six Flags Entertainment Corp.*, 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.[30]

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."[31] The second district did note, however, that an "injury or adverse effect need not be pecuniary."[32]

The Circuit Court of Cook County reached a different conclusion about the need to allege actual damages. In *Sekura v. Krishna Schaumberg Tan, Inc.*, Klaudi Sekura brought suit against Krishna Tan alleging that the company required its tanning customers to scan their fingerprints for identification purposes and that the company had not adequately informed her of its use of her fingerprint data.[33]

IN RECENT MONTHS, PLAINTIFFS HAVE SUED MORE THAN 30 COMPANIES ACROSS A RANGE OF INDUSTRIES FOR ALLEGEDLY VIOLATING BIPA.

Though this, too, was arguably just "a technical violation" – there was no allegation that Krishna Tan had allowed Sekura's biometric data to be compromised – the Circuit Court of Cook County found Sekura was "aggrieved" within the meaning of the statute.[34] The judge wrote that the term "aggrieved" does not require a plaintiff to plead "specific or actual damages" and is to be given a

20. *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088, 1102 (N.D. Ill. 2017).
21. *Id.*; see also *Monroy v. Shutterfly, Inc.*, No. 16-cv-10984, 2017 WL 4099846, at *6 (N.D. Ill. Sept. 15, 2017) (noting that Shutterfly could raise the issue at a later time when the record was clearer).
22. See *Monroy*, 2017 WL 4099846, at *7.
23. *Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103, 1105 (N.D. Ill. 2015).
24. *Gullen v. Facebook.com, Inc.*, No. 15-cv-7681, 2016 WL 245910, at *2 (N.D. Ill. Jan. 21, 2016).
25. *Spokeo Inc. v. Robins*, 136 S. Ct. 1540 (2016).
26. *McCollough v. Smarte Carte, Inc.*, No. 16-cv-3777, 2016 WL 4077108, at *3 (N.D. Ill. Aug. 1, 2016)
27. *Id.* at *4.
28. *Id.* at *3.
29. *Rosenbach v. Six Flags Entertainment Corp.*, 2017 IL App (2d) 170317, ¶ 21.
30. *Id.* at ¶ 1.
31. *Id.* at ¶ 28.
32. *Id.*
33. *Sekura v. Krishna Schaumberg Tan, Inc.*, No. 2016 CH 4945, at *1 (Ill. Cir. Ct. Feb. 9, 2017).
34. *Id.* at *2-3.

broad reading to protect "anyone like the plaintiff [] whose personal information has allegedly been mishandled in violation of BIPA...."[35] The court dismissed Krishna Tan's argument that this interpretation would allow plaintiffs "with no real injury" to bring BIPA lawsuits.[36]

**No 'biometric information' at stake.** 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.

## Conclusion

Recent months have seen an explosion in litigation under BIPA. With technology constantly evolving and advancing, particularly in the field of biometric information, BIPA will almost certainly be a topic of discussion and a source of litigation for years to come – a part of our dispute DNA.

35. *Id.* at *3.
36. *Id.*