THOMSON REUTERS
Westlaw®

Emerging issues and ambiguities under Illinois' Biometric Information Privacy Act

By Michael C. Andolina, Esq., Kathleen L. Carlson, Esq., Colleen T. Brown, Esq., Lawrence P. Fogel, Esq., Brian W. Tobin, Esq., and Andrew F. Rodheim, Esq., *Sidley Austin LLP*

MAY 21, 2020

In January 2019, the Illinois Supreme Court issued a seminal decision, *Rosenbach v. Six Flags Entertainment Corp.*,[1] holding that a plaintiff need not allege an actual injury or damages to successfully state a claim under Illinois' Biometric Information Privacy Act (BIPA),[2] which regulates the possession, collection and disclosure of biometric information.

Since *Rosenbach*, myriad cases alleging violations of BIPA have been filed in Illinois — and indeed around the country. And with its statutory penalties of $1,000 to $5,000 per violation, the potential exposure for defendants in these cases can be enormous.

For a statute that has received so much attention, there is a significant amount of uncertainty surrounding some of its most basic provisions.

This perhaps should not come as a surprise considering the brevity of the statute (only a few pages) and the limited number of cases that have reached a substantive decision on the merits.

Nonetheless, this uncertainty presents significant litigation risk to businesses that collect or otherwise possess biometric data of Illinois residents.

This article explores some of the more significant examples of ambiguity present in the statute and flags key issues of which all BIPA litigants — and indeed any company considering the implementation of biometric technology — should be aware.

The article concludes by providing concrete steps a company can take to reduce its potential liability under BIPA, which may in turn further mitigate liability on a larger scale given the increasing scrutiny of biometric privacy well beyond Illinois.

DO PLAINTIFFS HAVE FEDERAL STANDING IN BIPA ACTIONS?

A threshold issue frequently faced by BIPA litigants is whether the plaintiff has standing to bring the action.

At first glance, this question seemed to have been resolved by *Rosenbach*, in which the Illinois Supreme Court held that a plaintiff does not need to show actual harm to recover damages for BIPA violations. But the standing question is more complicated in federal court, where a plaintiff must suffer a particularized concrete injury-in-fact.

As the Supreme Court held in *Spokeo, Inc. v. Robins*,[3] a mere procedural violation is not enough.

This question of standing commonly arises when defendants remove a case to federal court and thus the parties are forced to adopt awkward arguments contrary to their ultimate positions on the merits.

The defendant, who as the removing party bears the burden of establishing that the federal court has jurisdiction, must argue that the plaintiff has suffered an injury-in-fact, while not conceding that the plaintiff is an "aggrieved person" within the meaning of BIPA.

And the plaintiff, who typically wants the case remanded to state court, must similarly walk the fine and uncomfortable line of arguing that she lacks standing because she has not alleged an injury-in-fact, without arguing that she has not suffered an injury under BIPA.

The awkwardness of this posture has not been lost on the courts. At least one court has suggested that "it is possible for the defendants to thread this needle."[4]

On May 5, 2020, the 7th U.S. Circuit Court of Appeals weighed in on this question.

In *Bryant v. Compass Group USA, Inc.*, the defendant had removed a BIPA action to the U.S. District Court for the Northern District of Illinois, and the plaintiff moved to remand, arguing (ironically) that she lacked standing because she had not alleged an injury-in-fact.[5]

The district court granted the plaintiff's motion, holding the plaintiff had alleged only a technical violation of BIPA, and not a "concrete injury" as required by Article III.

The 7th Circuit reversed, holding that plaintiff's BIPA § 15(b) claim conferred Article III standing. Section 15(b) imposes an informed consent requirement for the collection of biometric information.[6]

The court reasoned that the purpose of this provision, given the risk of identity theft or other privacy or economic harm related to disclosure of biometric information, "is to ensure that consumers

understand, before providing their biometric data, how that information will be used, who will have access to it and for how long it will be retained."[7]

Accordingly, the court determined that the defendant's collection of biometric data without informed consent "was not a failure to satisfy a purely procedural requirement."[8] The plaintiff "did not realize that there was a choice to be made and what the costs and benefits were for each option," the court said, ruling this deprivation was a concrete injury-in-fact sufficient to create Article III standing.[9]

On the other hand, the 7th Circuit held that the plaintiff did not have Article III standing to bring her BIPA § 15(a) claim. Section 15(a) requires that entities that possess biometric information establish a publicly available written retention and deletion policy.[10] The court reasoned that § 15(a) simply creates a duty to disclose to "the public generally," and therefore, the plaintiff alleged no particularized injury-in-fact resulting from the defendant's alleged violation of BIPA § 15(a).[11]

> Technology that merely identifies whether someone is male or female, or young or old, would likewise seem to fall outside of BIPA.

This case resolved a split among district court opinions in the Northern District of Illinois as to whether BIPA plaintiffs have Article III standing and was the first to draw a distinction between Sections 15(b) and 15(a) for purposes of standing.

WHAT DATA IS COVERED BY BIPA?

Another early question a BIPA litigant must answer is whether the biometric data the company unlawfully possessed, collected or disclosed is one of the "biometric identifiers" or "biometric information" regulated by BIPA.

BIPA Section 10 defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" while proceeding to specify a litany of data and contexts where biometric information would not constitute a biometric identifier.[12]

"Biometric information" is defined as data "based on an individual's biometric identifier" that is "used to identify an individual."[13] The legal obligations under BIPA apply to both biometric identifiers and biometric information.

Although these terms may seem straightforward, what qualifies as a biometric identifier in practice may in fact be more nuanced. Take, for example, a "voiceprint," which is not defined in BIPA. A company may then question: What, exactly, is a voiceprint and how is it distinct from a voice recording?

Logically, this cannot extend to all recordings of the human voice without ridiculous results, like imposing liability on any employer whose employee records their own voicemail greeting, or on all companies that make recordings of customer service calls.

But what about other voice recordings?

This question is at issue in an action pending in the Cook County Circuit Court, *Morales v. Google.com, Inc.*,[14] in which the plaintiffs allege that Google Assistant in-home devices recorded their voices in violation of BIPA.

Google filed a motion to dismiss arguing that the plaintiffs fail to state a cause of action because, among other reasons, a voice recording is distinct from a voiceprint and therefore is not covered by BIPA.

In support of its argument, Google pointed to a dictionary definition of voiceprint that limits the term to a physical representation of the human voice shown through a pattern of curved lines and whorls. The court has not yet ruled on Google's motion.

Another undefined and ambiguous biometric identifier under BIPA is "face geometry."

While some facial recognition technology is capable of and used to identify specific individuals, other technology is far more limited and used to identify more general characteristics, like gender or age. Does the latter qualify as biometric information under BIPA?

Although the courts have not yet addressed this question, the language of BIPA indicates the answer is no. The preamble to BIPA expressly notes that the Illinois Legislature's intent was driven by its finding that "biometrics [] are biologically unique to the individual."[15]

It is likely for this reason that the statute expressly excludes from its ambit "physical descriptions" that could equally apply to numerous individuals, "such as height, weight, hair color, or eye color."[16]

Technology that merely identifies whether someone is male or female, or young or old, would likewise seem to fall outside of BIPA.

Such arguments align with some of the core purposes of the law — to protect data that is immutable and, critically, an identifier for another human being at the most basic level.

THIRD PARTIES AND 'COLLECTION' VS. 'POSSESSION' OF BIOMETRIC INFORMATION

Another area of ambiguity concerns the potential liability of third parties who had no involvement in the collection of biometric information.

Take, for example, cloud storage companies that host data collected by other companies,[17] or third-party vendors

that provide and service technology that is later used by other companies to collect biometric information.[18] In each instance, these companies did not collect the biometric information, but later came into possession of it. What is their liability exposure under BIPA?

As an initial matter, BIPA does not expressly condition liability on whether an entity *knows* it possesses biometric information. However, a plaintiff must show that an entity violated the statute negligently, recklessly or intentionally to recover statutory damages.[19]

A cloud storage company in possession of data from myriad sources could plausibly argue that it has no liability under the statute because it lacked awareness that it possessed biometric information and lacked a duty to discover such data.

> Courts have recognized "there is a difference between possessing and collecting biometric information" for purposes of BIPA.

Some courts, however, have rejected this argument at the motion to dismiss stage, reasoning that the showing of intent relates to damages and not an element of the claim.[20]

BIPA does, however, explicitly impose different requirements on entities that "possess" and "collect" biometric data. Under § 15(a), entities that "possess" data must comply with BIPA's requirement to create a publicly available written retention and deletion policy as well as implement reasonable information security to protect the data.

In contrast, under Section 15(b), entities that "collect" data must comply with several additional steps, including informing the subject that it is collecting her biometric data, informing the subject of the purpose and length of time for which the biometric data is being collected and used, and obtaining the subject's written consent.

Plaintiffs often ignore this distinction and simply allege that third-party possessors violate both the possession *and* collection requirements of BIPA. Fortunately, however, courts have recognized "there is a difference between *possessing* and *collecting* biometric information" for purposes of BIPA.[21]

For example, in *Heard v. Becton, Dickinson & Co.*, the U.S. District Court for the Northern District of Illinois held that, unlike mere possession, the requirements in BIPA's collection provision apply only if an entity took "an *active step* to 'collect, capture, purchase, receive through trade, or otherwise obtain' biometric data."[22]

In that case, the plaintiff worked at several hospitals and was required to scan his finger in order to access a medication dispensing system. The plaintiff brought a BIPA claim against the manufacturer and seller of the medication dispensing system. Because the plaintiff did not explain how the defendant "collected" his data, and instead simply parroted BIPA's statutory language, the court dismissed his claim.[23]

WHAT IS A 'VIOLATION' UNDER BIPA?

Another question every BIPA defendant is likely to ask is, "What is my potential exposure?" BIPA states that an individual "aggrieved" by a violation of BIPA may recover $1,000 for "each" negligent violation and $5,000 for "each" intentional or reckless violation.

The statute does not, however, explain how to determine what "each" violation means.

As one example, consider a time clock featuring a finger reader, used by many companies to record when an employee clocks in and out of work each day. Does each scan, twice a day, constitute a potential violation, or is it limited to a single violation per person?

In *Peatry v. Bimbo Bakeries USA, Inc.*, the Northern District of Illinois evaluated, but did not resolve, this question. The court reasoned that BIPA "can plausibly be read to suggest that a violation ... allegedly occurred every time [an employee] clocked in and out of work."[24]

However, the court's discussion was limited to its evaluation of the amount-in-controversy requirement for federal diversity jurisdiction; it did not attempt to resolve the ambiguity and expressly left resolution for another day.

When that day does come, a plaintiff seeking the highest possible damages award could ask a court to draw parallels to the Telephone Consumer Protection Act (TCPA), a law that imposes statutory damages for certain unwanted phone calls and faxes.[25]

Specifically, plaintiffs could point to case law that calculates TCPA statutory damages on a per call or fax basis, as opposed to a per plaintiff basis, to argue BIPA imposes liability for each "use." However, the TCPA is infamous for abuse and is facing yet another Supreme Court challenge this term.[26]

Moreover, BIPA's prohibitions focus on acts of possession, collection and disclosure; meaningfully, BIPA does not mention "use" when defining the activity that may be a predicate for statutory liability.

This is so even though it is clear the Legislature contemplated that biometric information would be repeatedly "used," as it included within the definition of "biometric information" the requirement that the data be "used" for identification.

In short, if the Legislature sought to create separate statutory liability for each "use," it could have easily done so.

WHAT SHOULD A COMPANY DO TO PROTECT ITSELF AGAINST BIPA LIABILITY?

Given the proliferation of BIPA litigation and its many ambiguities, it is perhaps unsurprising that Illinois legislators from both sides of the aisle have recently introduced bills that may provide BIPA with needed limits and definition.[27]

However, until the Legislature acts or the courts provide clarity, companies should consider taking the following steps to reduce their potential liability under BIPA:

- Take inventory of existing biometric data. Any company that may have in the past possessed, collected or disclosed biometric identifiers of Illinois residents should undertake an investigation supervised by competent counsel to understand the extent of such possession or collection. This investigation should focus on and ensure that the data: (1) was collected in compliance with BIPA's notice and consent procedures; (2) is protected appropriately and in compliance with BIPA's requirements; and (3) will be destroyed when it is no longer needed for the original purpose for which it was collected, and in any event within three years of the individual's last interaction with the company.

- Minimize future collection and retention. Where possible, companies should limit any future collection and retention of biometric identifiers — broadly defined — of Illinois residents. While such collection and retention can increase efficiency and convenience for companies, employees and customers, it also poses significant legal risk and compliance cost.

- Follow notice and consent requirements. For future collection and retention of information, a company should immediately take steps to develop and publish a privacy policy relating to the company's handling of biometric identifiers, including a retention and deletion plan, and provide notice and obtain written consent for the handling of biometric data from all relevant Illinois residents. A company should also carefully consider whether to include arbitration clauses or class action waivers in applicable governing terms of use.

- Watch statutory developments in other states. Several states are considering biometric privacy laws either on their own or in conjunction with broader comprehensive privacy legislation.[28] Many of these laws could result in additional notice and consent requirements, if not use restrictions. Any deployment of a biometric data technology thus may be subject to evolving standards, not only in Illinois but across the country.

This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers. The content herein does not reflect the views of the firm.

Notes

[1] *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197 (Ill. 2019).

[2] 740 Ill. Comp. Stat. 14/1 *et seq.*

[3] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (holding, in a privacy harms case, that an injury in fact must be not only particularized but also "concrete").

[4] *Howe v. Speedway LLC*, No. 17-cv-07303, 2018 WL 2445541, at *3–4 (N.D. Ill. May 31, 2018).

[5] *Bryant v. Compass Group USA, Inc.*, No. 20-1443, 2020 WL 2121463 (7th Cir. May 5, 2020).

[6] 740 Ill. Comp. Stat. 14/15(b).

[7] *Bryant*, 2020 WL 2121463, at *7.

[8] *Id.*

[9] *Id.*

[10] 740 Ill. Comp. Stat. 14/15(a).

[11] *Bryant*, 2020 WL 2121463, at *7. The 9th Circuit has also addressed whether a BIPA plaintiff has Article III standing; it held that the plaintiff had Article III standing to bring both his § 15(a) and § 15(b) claims. *See Patel v. Facebook, Inc.*, 932 F.3d 1264, 1275 (9th Cir. 2019) ("Because we conclude that BIPA protects the plaintiffs' concrete privacy interests and violations of the procedures in BIPA actually harm or pose a material risk of harm to those privacy interests, the plaintiffs have alleged a concrete and particularized harm, sufficient to confer Article III standing.") (citation omitted), *cert. denied*, 140 S. Ct. 937 (2020).

[12] 740 Ill. Comp. Stat. 14/10.

[13] *Id.*

[14] No. 2019-ch-08309 (Ill. Cir. Ct., Cook Cty.).

[15] 740 Ill. Comp. Stat. 14/5.

[16] 740 Ill. Comp. Stat. 14/10.

[17] *See, e.g., Ragsdale v. Amazon Web Services, Inc.*, No. 2019-ch-13251 (Ill. Cir Ct., Cook Cty.).

[18] *See, e.g., Heard v. Becton, Dickinson & Co.*, No. 19-cv-4158, 2020 WL 887460 (N.D. Ill. Feb. 24, 2020); *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279 (N.D. Ill. 2019); *Bernal v. ADP, LLC*, No. 2017-ch-12364, 2019 WL 5028609 (Ill. Cir. Ct., Cook Cty. Aug. 23, 2019).

[19] *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1104 (N.D. Ill. 2017) (citing 740 Ill. Comp. Stat. 14/20).

[20] *See, e.g., Peatry v. Bimbo Bakeries USA, Inc.*, No. 19-cv-2942, 2020 WL 919202, at *6 (N.D. Ill. Feb. 26, 2020) (citing *Woodard v. Dylan's Candybar LLC*, No. 2019-ch-05158, at *9 (Ill. Cir. Ct., Cook Cty. Nov. 20, 2019)).

[21] *Namuwonge*, 418 F. Supp. 3d at 286; *see also, e.g., Heard*, 2020 WL 887460, at *3; *Bernal*, 2019 WL 5028609, at *1; *but see, e.g., Figueroa v. Kronos Inc.*, No. 19-cv-1306, 2020 WL 1848206, at *5–6 (N.D. Ill. Apr. 13, 2020); *Neals v. Par Tech. Corp.*, No. 19-cv-5660, 2019 WL 6907995, at *1 (N.D. Ill. Dec. 18, 2019).

[22] *Heard*, 2020 WL 887460, at *4 (emphasis added) (quoting 740 Ill. Comp. Stat. 14/15(b)).

[23] Similarly, in *Bernal v. ADP, LLC*, an Illinois Chancery Court dismissed a BIPA claim against a third party that was responsible only for providing and servicing a time clock using biometric scanning technology. 2019 WL 5028609, at *1–2 ("[T]here is nothing to suggest that BIPA was

intended to apply to situations wherein the parties are without any direct relationship.").

[24] *Peatry v. Bimbo Bakeries USA, Inc.*, 393 F. Supp. 3d 766, 769 (N.D. Ill. 2019).

[25] 47 U.S.C.A. § 227.

[26] *Barr v. Am. Ass'n of Political Consultants Inc.*, No. 19-631, *argument held*, 2020 WL 2226264 (U.S. May 6, 2020).

[27] SB3776, introduced by Democratic Sen. Bill Cunningham on Feb. 14, 2020, would limit BIPA recovery to actual damages where the "offending party" is the current or former employer of the prevailing party. SB3592 and SB3593, introduced by Republican Sen. Jason A. Barickman on the same day, would alternatively eliminate or qualify the private right of action in BIPA.

[28] For example, Washington state has introduced the Washington Privacy Act, which among other things, would impose increased restrictions related to biometric data. *See* Washington SB 6281.

This article appeared on the Westlaw Practitioner Insights Commentaries web page on May 21, 2020.

ABOUT THE AUTHORS






(L-R) **Michael C. Andolina** is a partner in **Sidley Austin**'s Chicago office and is a deputy group head of the Chicago Litigation group. His practice focuses on working with clients to manage crises and resolve complex multiparty and multi-jurisdiction matters. He can be reached at mandolina@sidley.com. **Kathleen L. Carlson** is a partner in the firm's Chicago office who focuses on class action defense and commercial litigation and disputes. She can be reached at kathleen.carlson@sidley.com. **Colleen T. Brown** is a partner in the firm's Washington office. Her practice focuses on privacy, cybersecurity, data protection and emerging technology issues. She can be reached at ctbrown@sidley.com. **Lawrence P. Fogel**, **Brian W. Tobin** and **Andrew F. Rodheim** are associates in the Litigation group of Sidley's Chicago office and members of its Commercial Litigation and Disputes group.