PAUL HASTINGS

STAY CURRENT

May 2020

Follow @Paul_Hastings

Seventh Circuit Lowers the Federal Standing Threshold for Illinois Biometric Privacy Act Claimants

By Aaron Charfoos, Behnam Dayanim, Adam Reich & Matthew Lind

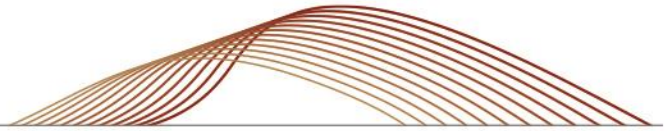
This week, the Seventh Circuit Court of Appeals issued a decision that opens the door to more frequent federal court determination of statutory claims under the Illinois Biometric Information Privacy Act, 740 ILCS 14/1–99 ("BIPA"). In *Bryant v. Compass Group USA, Inc.*, No. 20-1443, the court considered whether federal standing requirements under Article III of the U.S. Constitution were met by a technical violation of BIPA's provisions requiring informed written consent to collect and store a person's fingerprint. Drawing on "the sensitivity of biometric information and the risk of identity theft or other privacy or economic harm that may result from its dissemination," the court concluded that even a technical BIPA violation can deprive people of "the opportunity to make informed choices about to whom and for what purpose they will relinquish control of that information."[1] This decision invites both plaintiffs and defendants to litigate more BIPA claims in federal courts, rather than in Illinois state courts, and may portend more widespread federal litigation of BIPA claims nationwide.

BIPA

In 2008, the Illinois Legislature passed BIPA to "regulat[e] the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[2] BIPA "is designed to protect consumers against the threat of irreparable privacy harms, identity theft, and other economic injuries arising from the increasing use of biometric identifiers and information by private entities.https://www.paulhastings.com/publications-items/details/?id=3b81716c-2334-6428-811c-ff00004cbded - edn5"[3] Under BIPA, "biometric information" is defined as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[4]https://www.paulhastings.com/publications-items/details/?id=3b81716c-2334-6428-811c-ff00004cbded - edn6 Biometric information is limited to "information derived from items or procedures" included in the definition of biometric identifiers, such as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[5]

In order to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information," BIPA, in its section 15(b), requires that the private entity attempting to collect, purchase, receive, or otherwise obtain such information:

1. [inform] the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;



2. [inform] the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

3. [receive] a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.[6]

Under section 15(a) of the statute, BIPA also separately requires a private entity that possesses biometric identifiers or information to develop and make public a written policy "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 three years of the individual's last interaction with the private entity, whichever occurs first."[7]

BIPA provides a private right of action to any person "aggrieved by a violation" of BIPA, whereby such a person may seek damages, attorney's fees and costs, and injunctive relief.[8]

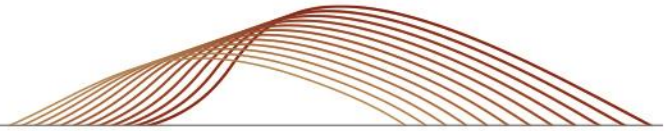
The *Bryant* Opinion

In *Bryant*, a call-center employee filed a class-action lawsuit in the Cook County Circuit Court in the State of Illinois against Compass Group USA ("Compass"), claiming that Compass violated BIPA's informed-consent requirement (section 15(b) of BIPA) when it mandated that employees provide fingerprints to use vending machines without first or concurrently informing the employees that, or for how long, their fingerprints would be collected and stored, and also without obtaining a written release from each employee to collect, store, and use their fingerprints. Bryant further alleged that Compass failed to publicly disseminate a retention and destruction policy for the fingerprints it collected and stored, in violation of section 15(a) of BIPA.

Compass removed the suit to federal court under the federal Class Action Fairness Act, 28 U.S.C. § 1332(d). Bryant sought a remand order by asserting that the alleged injury—technical violations of BIPA's informed-consent and written-policy requirements—do not support the "aggrieved" party standing requirement of Article III of the U.S. Constitution. The United States District Court for the Northern District of Illinois agreed with Bryant's position and remanded the case to state court.[9] Compass appealed the remand order.

In a long-awaited opinion, the Seventh Circuit Court of Appeals reversed the District Court's remand order. Specifically, the Seventh Circuit held that the mere violation of BIPA's informed-consent provisions (section 15(b)'s so-called "heart of BIPA"[10]), constitutes a sufficient injury to support Article III standing because such violation "denied Bryant and others like her the opportunity to consider whether the terms of [biometric-information] collection and usage were acceptable given the attendant risks."[11] The Seventh Circuit explained its conclusion by noting that Compass's alleged failure to "make the requisite disclosures to Bryant or obtain her informed written consent before collecting her fingerprints, . . inflicted the concrete injury BIPA intended to protect against, i.e. a consumer's loss of the power and ability to make informed decisions about the collection, storage, and use of her biometric information."[12]

In contrast to its conclusion concerning standing for informed consent litigation under section 15(b), the Seventh Circuit also held that a violation of BIPA's written-policy requirement (section 15(a)) does not confer standing on individuals.[13] The court reasoned that BIPA's requirement that companies publish their data-retention schedule and guidelines for destroying collected biometric information



constitutes a duty "owed to the public generally, not to particular persons whose biometric information the entity collects."[14] As such, the Seventh Circuit concluded, a mere violation of that requirement did not cause a "concrete and particularized injury" that would independently support Article III standing.[15]

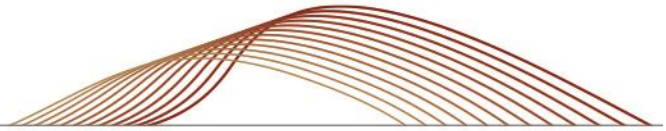
Bryant May Have a Significant Impact on BIPA Litigation

Many legal commentators believe that the impact of the Seventh Circuit's Opinion in *Bryant* has a chance to be wide-ranging and fundamental. First, as *Bryant* removes a procedural standing hurdle necessary for a case brought under section 15(b) of BIPA to proceed in federal courts in the Seventh Circuit, there is likely to be an uptick in BIPA lawsuits filed in and removed to federal courts, particularly in the Northern District of Illinois, where so many businesses are based and the plaintiff's bar is particularly active. Second, the *Bryant* opinion may result in a decrease of BIPA lawsuits filed in the Ninth Circuit, which previously stood alone in holding (similar to the Seventh Circuit in *Bryant*) that Article III standing may be found even where only a procedural violation of BIPA has occurred,[16] and, more broadly, that any violation of a privacy statute is sufficient to confer Article III standing even if the plaintiff cannot show a tangible injury. [17] Third, the adoption of this relaxed standing viewpoint by a second United States Circuit Court of Appeals may foreshadow a trend across the country with respect to privacy litigation more generally, whether under BIPA or other privacy statutes.

Still, it cannot be lost that the Seventh Circuit in *Bryant* expressly distinguished technical violations of BIPA's written policy provision (section 15(a)) from technical violations of BIPA's informed-consent provision (section 15(b)), finding the former to be insufficient to confer Article III standing. In so doing, the Seventh Circuit has confirmed a definitive viewpoint that not all statutory violations will automatically constitute grounds to pursue BIPA litigation in federal court. *Bryant* therefore stops short of the implicit rule endorsed by the Ninth Circuit that even technical violations of BIPA's section 15(a) can confer Article III standing.[18] Ultimately, this may lead to a bifurcation of BIPA lawsuits in the Seventh Circuit, with claims under section 15(b) pursued in federal court and claims under section 15(a) litigated in state courts.[19]

The Seventh Circuit's *Bryant* Opinion comes at a unique time. COVID-19 has resulted in numerous legal and policy changes, both at governmental and corporate levels which implicate privacy concerns.[20] Employees, consumers, and the plaintiff's bar have shown themselves to be attuned to these changes, and there has been a noticeable uptick in consumer class action filings brought under privacy statutes. In this environment, and considering that even before COVID-19, an increasing number of class action lawsuits had been filed under BIPA, over the last several years, it is likely that this upward trend in BIPA litigation will accelerate.

Over the coming months and years, companies must be attentive to their privacy policies and practices, and those of their vendors, as converging legal, social, and technological forces are increasing exposure to class-action litigations under BIPA and other privacy statutes in both state and federal courts. Paul Hastings remains uniquely positioned to aid in the review and revision of biometric information collection and retention policies, and can draw on its wealth of experience to capably guide clients through emerging data-privacy challenges. Our Chicago legal team's experience navigating BIPA and other privacy issues is supported by Paul Hastings' nationally unique and cross-disciplinary team of legal and regulatory experts—including a former U.S. Department of Homeland Security cyber-policy expert, high-profile privacy and security officers of Fortune 100 companies, and Ph.D.-credentialed data scientists with diverse perspectives and experiences in business, law, and technology.



✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

Matt Lind
1.312.499.6062
mattlind@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Mark D. Pollack
1.312.499.6050
markpollack@paulhastings.com

Adam M. Reich
1.312.499.6041
adamreich@paulhastings.com

---

[1] *Bryant v. Compass Group USA, Inc.*, No. 20-1443, at 15–16 (7th Cir. May 5, 2020).

[2] 740 ILCS 14/5(g).

[3] *Bryant* at 1–2.

[4] 740 ILCS 14/10.

[5] *Id.* Notably, BIPA expressly excludes from biometric identifiers: "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." *Id.*

[6] 740 ILCS 14/15(b).

[7] 740 ILCS 14/15(a).

[8] 740 ILCS 14/20.

[9] Following the Illinois Supreme Court's decision last year in *Rosenbach v. Six Flags Entertainment Corp.*, Illinois courts have been less stringent in finding standing thresholds satisfied. *See* B. Dayanim et al., Rosenbach v. Six Flags Entertainment Corp.: The Illinois Supreme Court Clarifies BIPA's "Aggrieved" Pleading Requirement, Paul Hastings Insights (Feb. 6, 2019).

[10] *Bryant* at 15.

[11] *Id.* at 16.

[12] *Id.* at 17.

[13] *Id.* at 16.

[14] Id.

[15] *Id.* at 17.

[16] See *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1275 (9th Cir. 2019) (finding a "concrete and particularized harm" for procedural violations because "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").

[17] *See Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1118 (9th Cir. 2020) (finding that "*every* violation" of certain privacy statutes constitutes an actionable concrete harm) (emphasis in original).

[18] *See Patel*, 932 F.3d at 1274 (finding that "Facebook's alleged violation of these statutory requirements [under sections 15(a) and 15(b)] would necessarily violate the plaintiffs' substantive privacy interests" and constitute "a concrete injury-in-fact sufficient to confer Article III standing").

[19] *See Bryant* at 17 (finding that Bryant "lack standing under Article III to pursue [her section 15(a)] claim in federal court," but that "Bryant's claim under section 15(b) may proceed in federal court").

[20] *See* Konrad Putzier & Chip Cutter, Welcome Back to the Office. Your Every Move Will be Watched, THE WALL STREET JOURNAL, May 5, 2020.