Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Ill. Biometric Privacy Ruling Is Only The Beginning For BIPA

By **Al Saikali, Tristan Duncan and Gary Miller** (January 29, 2019, 5:00 PM EST)

Al Saikali

Tristan Duncan

Gary Miller

The Illinois Supreme Court's decision last week in Stacy Rosenbach v. Six Flags Entertainment Corp. may have closed the first of what will be several chapters in class action litigation arising from the Illinois Biometric Information Privacy Act. The court addressed the very narrow issue of what it means for a person to be "aggrieved" under BIPA. Ultimately, the court held that a violation of the notice, consent, disclosure or other requirements of BIPA alone, without proof of actual harm, is sufficient for a person to be considered "aggrieved" by a violation of the law.

There are several important issues, however, that were not before the court and remain to be litigated. One of those issues is constitutional standing. Federal courts have recently dismissed BIPA lawsuits on the ground that they do not meet Article III standing requirements.[1] Defendants in state court will argue that Illinois constitutional standing (which Illinois state courts have held should be similar to federal law) requires a level of harm that, at a minimum, should be what Article III of the U.S. Constitution requires.[2] To hold otherwise would lead to a different result for a party based entirely on whether the lawsuit is filed in federal or state court.

Defendants will also argue that most of the claims are barred by the one-year statute of limitations that applies to claims involving the right of privacy. Assuming that the one-year statute of limitations is applied, the classes of affected individuals will shrink considerably.

Another significant defense is implied notice and consent. Defendants will argue that the plaintiffs who checked in/out at work using finger scan timekeeping systems (which is the fact pattern of almost all of the almost 200 class actions filed in state court) knew that the finger scans were being collected and used by their employers for timekeeping purposes, and they voluntarily provided that information. Federal courts have dismissed such lawsuits, reasoning that plaintiffs effectively received notice and gave consent.

In Howe v. Speedway LLC,[3] for example, the court in a finger scan timekeeping case held that the plaintiff's "fingerprints were collected in circumstances under which any reasonable person should have

known that his biometric data was being collected." Similarly, in Santana v. Take-Two Interactive Software Inc.,[4] the U.S. Court of Appeals for the Second Circuit held that plaintiffs essentially received the notice and consent contemplated by BIPA because "the plaintiffs, at the very least, understood that Take-Two had to collect data based upon their faces in order to create the personalized basketball avatars, and that a derivative of the data would be stored in the resulting digital faces of those avatars so long as those avatars existed." In dismissing for lack of standing, the McGinnis court reasoned that the plaintiff "knew his fingerprints were being collected because he scanned them in every time he clocked in or out of work."

Defendants will also argue that the information collected/stored by the timekeeping devices is not considered biometric information under BIPA. There is no library of fingerprints stored by these timekeeping devices. Instead, the devices measure minutiae points and convert those measurements into mathematical representations using a proprietary formula that cannot be used to create a fingerprint. More security is layered on top of that — the mathematical representation is encrypted. For these reasons, no plaintiff in any of these biometric cases has been able to point to a single data breach involving biometric information. The technology is essentially tokenization (similar to Apple Pay), where if a hacker were to access the actual device, he'd find nothing there to steal because the valuable thing (the credit card number or, in this case, fingerprint) is not stored on the device but is instead replaced by a numerical representation.

Plaintiffs will also have to prove that the defendants didn't just violate BIPA, but did so negligently or intentionally. This is not an easy standard to meet, especially if the trier of fact determines that these are "gotcha" lawsuits, meant to catch companies off-guard about a little known and rarely used state law.

Assuming the plaintiffs jump all these hurdles, they must still demonstrate that these cases are appropriate for class certification. The cases involve different facts regarding whether individual plaintiffs received notice, whether they gave consent, whether they used the finger scan method of authentication or another method like PIN number or RFID card, whether they enrolled in Illinois, and whether their claim involves a violation of BIPA beyond collection or storage. Given these differences between plaintiffs, it will be difficult for them to meet the commonality and fairness requirements for class certification.

To be sure, some defendants will face their own challenges. A line of cases has held that where companies used their time-clock provider's cloud service to store or back up timekeeping information from the clock, they may be in violation of BIPA's prohibition against disclosure of biometric identifiers to a third party.[5] But at least one court has disagreed with that logic, stating that not all disclosures to a third party automatically present a concrete injury, and whether the third party has strong protocols and practices in place to protect data is relevant to the inquiry.[6]

Defendants need only win one of these (or several other) defenses. Plaintiffs must win them all. In the meantime, plaintiffs must hope that the Illinois Legislature does not notice that hundreds of BIPA lawsuits are flooding the Illinois state court system, creating potentially crippling liability for companies that tried to adopt more secure methods of authentication, which could lead to an amendment that would make the law more consistent with its original intent.

Al Saikali chairs the privacy and data security practice at Shook Hardy & Bacon LLP.
Tristan Duncan co-chairs the firm's class action practice.
Gary Miller co-chairs the firm's business litigation practice.

Disclosure: Shook Hardy represents companies in BIPA class actions and filed an amicus brief in Rosenbach v. Six Flags in the Illinois Supreme Court.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See, e.g., McGinnis v. U.S. Cold Storage, Inc., No. 17C8054 (N.D. Ill. Jan. 3, 2019); Rivera v. Google, Inc., No. 16C2714 (N.D. Ill. Dec. 29, 2018).

[2] See Maglio v. Advocate Health & Hosps. Corp., 2015 IL App (2d) 140782, 25-26 ("Federal standing principles are similar to those in Illinois, and [federal] case law is instructive.").

[3] Howe v. Speedway LLC, 2018 WL 2445541, at *6 (N.D. Ill. May 31, 2018)

[4] Santana v.Take-Two Interactive Software Inc., 717 F. App'x 12 (2d Cir. 2017)

[5] See Dixon v. Washington & Jane Smith Cmty., 2018 WL 2445292 (N.D. Ill. May 31, 2018).

[6] See McGinnis, at *4