Legal Opinion Letter

Vol. 27 No. 17 November 16, 2018

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

Biometric Privacy Case before Illinois Supreme Court Could Open Litigation Floodgates

by Kwabena A. Appenteng and Philip L. Gordon

On November 20, 2018, the Illinois Supreme Court will hear oral arguments in a case that has significant implications for Illinois employers, though it is not an employment-law case. Over the past two years, more than 100 class action lawsuits have been filed by employees under the Illinois Biometric Information Privacy Act ("BIPA"). The employees claims that their employer utilized a biometric timeclock[1] without complying with two BIPA requirements: (1) providing a written notice explaining the purpose of collecting, and the retention period for, the biometric data; and (2) obtaining employees' written consent to the data collection. Because BIPA provides that "any person *aggrieved by* a violation of th[e] Act shall have a right of action," the complaints in these cases allege that each employee in the putative class is entitled to recover statutory damages of at least $1,000 without pleading or proving actual harm.

On December 21, 2017, an Illinois appeals court rejected this theory, ruling that a private entity's failure to comply with BIPA's notice-and-consent requirements, without any allegation of actual harm, is nothing more than a "technical violation" for which a plaintiff cannot obtain relief. *See Rosenbach v. Six Flags Entertainment Corp.*, 2017 IL App (2d) 170317, ¶¶ 23, 28. The court made clear: "Alleging only technical violations of the notice and consent provisions of the statute, as plaintiff did here, does not equate to alleging an adverse effect or harm." *Id.* at ¶21. The Illinois Supreme Court allowed plaintiff's petition for leave to appeal on May 30, 2018.[2]

Within the next few months, that court will decide whether an individual can obtain statutory damages or injunctive relief under BIPA when the only "injury" alleged is a violation of BIPA's notice-and-consent requirements. In order for the court to answer that question, however, it likely will need to address several important underlying issues, and consider the potential ramifications of its ruling. This Legal Opinion Letter outlines the issues the court may need to consider.

Issue #1: *BIPA's Legislative Intent*. BIPA was enacted after Pay By Touch, the largest fingerprint scan system in Illinois, filed for bankruptcy, and the bankruptcy court approved the sale of Pay By Touch's database of biometric data. *See* 740 ILCS 14/5 ("Legislative findings; intent"). At least one Illinois federal court has determined that the legislature's intent in enacting BIPA was to "create a legal right to privacy in personal biometric data and to protect the right to control one's biometric identifiers and information," in support of its holding that actual harm need not be alleged to state a claim. *Dixon v. The Washington and Jane Smith Community*, No. 17-cv-08033, 2018 WL 2445292 (N.D. Ill. May 31, 2018).

The Illinois Supreme Court must first examine what the legislature intended on the question of injury. If the court were to recognize that BIPA creates a right of privacy, the court likely would rule that employees

[1] A biometric timeclock is timekeeping technology that uses a scan of an employee's body feature, such as a fingerprint, retina or iris, to verify the employee's identity and clock the employee into, and out of, work.

[2] *Rosenbach v. SixFlags Entertainment Corp.*, No. 123186.

Kwabena A. Appenteng is a Senior Associate with Littler Mendelson P.C. in the firm's Chicago, IL office, and **Philip L. Gordon** is a Shareholder in the firm's Denver, CO office.

who knowingly provide biometric data using the employer's biometric timeclock without receiveing notice or giving consent can state a claim even without pleading any actual harm.

Issue #2: ***Federal Court Rulings***. Over the past two years, several federal district courts have ruled that an employee claiming a mere violation of BIPA's notice-and-consent requirements has not suffered an injury-in-fact sufficient to support federal jurisdiction. Notably, a number of these cases involved biometric timeclocks.[3] Although the Illinois Supreme Court is not bound by these rulings, the court is likely to address them, as state appellate courts commonly consider relevant federal court authority on state-law concerns.

Issue #3: ***Potential Spike in BIPA Class Actions against Employers***. Though businesses are also being sued over consumer-based biometric technology, the plaintiffs' bar has especially targeted workplace timeclocks. A fingerprint scanner that signs a customer into his local tanning salon, or a facial recognition scanner that allows a consumer to access her profile at a fast-food restaurant,[4] for instance, may be used only two or three times a month. Those same businesses' biometric timeclocks, by comparison, will typically be used at least four times a day, five days a week, by a full-time, non-exempt employee. This frequent use of biometric technology in the workplace, coupled with the number of employees whose biometric data is captured each day, has inspired the plaintiffs' bar to target businesses as employers. Employees can conceivably assert that BIPA entitles them to at least $1,000 in statutory damages for each time biometric data is collected without notice and consent. If the Illinois Supreme Court were to decide that those statutory violations, standing alone, are enough to sustain a BIPA action, employers are almost certain to see an increase in BIPA litigation.

Issue #4: ***Unforeseeable Liability***. At present, the law itself provides the only guidance that exists on calculating damages under BIPA. The law permits the following recovery for violations: (1) where a private entity "negligently" violates BIPA, the greater of $1,000 per violation, or actual damages; and (2) where a private entity "recklessly violates" BIPA, the greater of $5,000 per violation, or actual damages. The question then becomes what constitutes a "violation" for purposes of the statute.

The most logical reading would be that an employer's failure to provide notice and obtain consent constitutes only one violation for each employee whose biometric data was collected. However, as noted above, some class action complaints appear to be seeking a measure of damages that would result in an award of statutory damages *each time* an employer collected biometric data from each employee without notice or consent. Given that many non-exempt employees clock in and out several times each day, such a method of calculation could result in potentially crippling liability for many businesses. The inability to accurately project potential exposure in BIPA litigation—at least until this issue is resolved—potentially is a significant concern for publicly traded companies and even for smaller companies trying to engage in forward-looking planning.

Conclusion. Regardless of how the Illinois Supreme Court rules, its decision will have significant consequences for Illinois employers. As employers await the court's ruling in *Rosenbach*, they should use the time to evaluate their BIPA-compliance efforts.

---

[3] *See, e.g., Howe v. Speedway,* No. 17-cv-7303, 2018 WL 2445541 (N.D. Ill. May 31, 2018) (holding employee who alleged he did not receive a written notice or provide written consent before using a biometric timeclock had not demonstrated they suffered an injury-in-fact, and noting that it was "readily apparent" to the employee that his fingerprint was being scanned and stored and "proper compliance with BIPA's disclosure and written authorization requirements would only have made explicit what should have already been obvious"); *Goings v. UGN, Inc.*, No. 17-cv-9340, 2018 WL 2966970 (N.D. Ill. Jun. 13, 2018) (holding employee's allegations that he used a biometric timeclock without first receiving a written notice or giving written consent did not demonstrate an injury-in-fact and noting that the employee was aware that he was providing his biometric data); *Aguilar v. Rexnord LLC*, No. 17-cv-9019, 2018 WL 3239715 (N.D. Ill. Jul. 3, 2018) (holding "notice and consent violations do not without more create a risk of disclosure, and [the employee] knew his biometric information was being collected, even though he did not receive formal notice and give formal consent").

[4] *See* Leslie Wu, *Big Burger Is Watching You, and Other Ways Facial Recognition Software Is Entering Foodservice*, Forbes.com (Dec. 31, 2017), https://www.forbes.com/sites/lesliewu/2017/12/31/big-burger-is-watching-you-and-other-ways-facial-recognition-software-is-entering-foodservice/#7b1fc8336c4d.

 ISBN 1056 3059