AN A.S. PRATT PUBLICATION
APRIL 2019
VOL. 5 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Collecting Biometric Information Just Became Riskier Under Illinois Law

Patrick J. Burke and Alisha L. McCarthy*

The authors of this article discuss a recent Illinois Supreme Court ruling, which is a boost to plaintiffs in Biometric Information Privacy Act lawsuits, and carries a cautionary note for companies that collect biometric information from consumers or employees in Illinois.

The Illinois Supreme Court recently ruled that individuals need not suffer actual harm in order to sustain claims under Illinois's Biometric Information Privacy Act.[1] The ruling, issued in *Rosenbach v. Six Flags Entertainment Corp.*,[2] is a boost to plaintiffs in BIPA lawsuits, and carries a cautionary note for companies that collect biometric information from consumers or employees in Illinois.

BIPA, which was enacted in 2008, requires companies to obtain consent from individuals before collecting or storing biometric information such as fingerprints, retina or iris scans, voiceprints, and hand and face geometry. BIPA authorizes courts to award monetary damages to any person "aggrieved" by a violation of the Act.

The Act has prompted a spate of litigation, including class actions by employees against their employers, and by consumers against tech giants like Facebook and Google. Courts have split on the question of whether plaintiffs can sue for violations of the Act without alleging actual injuries – such as identity theft or pecuniary loss – arising from the violations. The decision in *Rosenbach* settled that question in favor of the plaintiff.

ROSENBACH V. SIX FLAGS ENTERTAINMENT CORP.

The *Rosenbach* case arose after Six Flags scanned the thumbprint of Alexander Rosenbach, a minor, to set up a season pass at one of their amusement parks. Alexander's mother, Stacy, signed him up online for the season pass before a school field trip, but did not accompany her son to the park. When Alexander arrived at the park he was asked to scan his thumb into the Six Flags biometric data capture system to set

* Patrick J. Burke is a partner at Phillips Nizer LLP, where he heads the firm's Data Technology & Cybersecurity Practice Group. Mr. Burke is the former Deputy Superintendent, Office of Financial Innovation, New York State Department of Financial Services, where he oversaw policy and examination of New York's licensed and chartered financial institutions, pursuant to the department's cybersecurity and virtual currency regulations, including crypto-currency and blockchain innovations. Alisha L. McCarthy is an associate in the firm's litigation department. The authors may be reached at pburke@phillipsnizer.com and amccarthy@phillipsnizer.com, respectively.

[1] 740 ILCS 14/1 et seq. ("BIPA").

[2] 2019 IL 123186 (Jan. 25, 2019).

up the season pass. Upon his return home, his mother asked to see the paperwork provided in connection with the pass, and learned that none had been provided because Six Flags did "it all by fingerprint now."

Stacy Rosenbach sued on behalf of her son, alleging that Six Flags had violated BIPA by collecting and storing Alexander's thumbprint without informing Alexander or his mother of the specific purpose for which his fingerprint had been collected and length of time for which it would be stored, and without obtaining prior consent.

Illinois's highest court, analyzing the statute, determined that Rosenbach was not required to allege actual injury to proceed against Six Flags: alleging a violation of the Act was sufficient to give Rosenbach standing as an "aggrieved" person under BIPA. The court reasoned that when "a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, the right of the individual to maintain his or her biometric privacy vanishes into thin air. . . ."[3] According to the Illinois Supreme Court, such a violation of the Act "is no mere 'technicality.' The injury is real and significant."[4] The court elaborated: "To require individuals to wait until they have sustained some compensable injury beyond violation of their statutory rights before they may seek recourse . . . would be completely antithetical to the Act's preventative and deterrent purposes."[5]

PREDICTIONS AND GUIDANCE AFTER *ROSENBACH*

The *Rosenbach* decision may open the floodgates of BIPA litigation against entities that collect and store biometric data from Illinois consumers. Class action litigation can be particularly attractive given the statute's provision for liquidated damages of $1,000 to $5,000 per aggrieved individual, plus attorney's fees and costs.

Class action targets have included employers who use biometrics for security and timeclock purposes, and technology companies like Google and Facebook. Google was sued in a putative class action in the U.S. District Court for the North District of Illinois, in which plaintiffs alleged that Google unlawfully collected, stored, and exploited face-geometry scans via Google Photos. Google had the case dismissed, based on the argument that plaintiffs had not suffered injury. Facebook, on the other hand, was unable to obtain dismissal on those grounds in a putative federal class action in the U.S. District Court for the Northern District of California, in which plaintiffs have alleged that Facebook's "Tag Suggestion" program extracts and stores biometric identifiers from photographs that users upload.

[3] *Id.* ¶ 34 (quotation and internal alteration omitted).
[4] *Id.* ¶ 34.
[5] *Id.* ¶ 37.

Private entities should take steps to ensure full compliance with the letter and spirit of the Act. Among other things, BIPA prohibits the collection or retention of biometric information without first:

(i) Informing the subject that the information is being collected;
(ii) Informing the subject of the specific purpose of the collection and the length of time the information is to be stored/used; and
(iii) Receiving a written release executed by the subject or their legally authorized representative.

BIPA also requires covered entities, under certain circumstances, to "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information. . . ." Further, a company in possession of biometric information must store, transmit, and protect from disclosure all biometric identifiers and information "using the reasonable standard of care within the private entity's industry," and in a manner "that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." Companies should consult with counsel and implement standardized processes and policies to satisfy these and the other requirements of the Act.