Intellectual Property & Technology Law Journal

Edited by the Technology and Proprietary Rights Group of Weil, Gotshal & Manges LLP

VOLUME 31 • NUMBER 4 • APRIL 2019

Rosenbach v. Six Flags — Illinois Supreme Court Takes Expansive View of Statutory Standing Under the Biometric Information Privacy Act

By Kathryn E. Deal, Meredith C. Slawe, Natasha G. Kohne, and Michelle A. Reed

The Illinois Supreme Court recently issued a unanimous decision interpreting Illinois' Biometric Information Privacy Act[1] (the BIPA). In the closely-watched *Rosenbach v. Six Flags Entertainment Corp.* appeal, the court concluded that a plaintiff does not need to plead actual harm or injury resulting from an alleged BIPA violation in order to seek injunctive relief and liquidated statutory damages of up to $5,000 per alleged violation. In reaching this conclusion, the court overruled the intermediate appellate court, which had found that a mere technical violation of the BIPA was insufficient to confer standing to sue because the statute expressly requires an individual to be "aggrieved" by a statutory violation before he or she has a private right of action.

The court's decision is inconsistent with the approach to constitutional standing employed in federal courts, and it also departs from other judicial interpretations of what it means to be "aggrieved" by an alleged statutory infraction. As a result, given the growing use of biometric technology, companies operating in Illinois should be aware of the *Rosenbach* ruling and the potential it has to perpetuate state court litigation and disproportionate aggregate exposure under the BIPA, even in the absence of any identified loss, data breach, or actual damage.

Background

The BIPA was enacted in 2008 in response to the growing "use of biometrics" in "financial transactions and security screenings."[2] Specifically, the statute governs private entities that possess biometric identifiers and/or biometric information. The BIPA defines biometric

Kathryn E. Deal (*kdeal@akingump.com*) is a partner at Akin Gump Strauss Hauer & Feld LLP representing corporate and institutional clients in class action and commercial litigation nationwide. **Meredith C. Slawe** (*mslawe@akingump.com*) is a partner at the firm defending companies in consumer class actions and commercial cases in federal and state courts. **Natasha G. Kohne** (*nkohne@akingump.com*) is a partner at the firm and co-leader of the firm's cybersecurity, privacy, and data protection practice. **Michelle A. Reed** (*mreed@akingump.com*) is a partner at the firm and co-leader of the firm's cybersecurity, privacy, and data protection practice.

identifiers to include "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[3] In turn, the statute defines biometric information 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]

The BIPA was enacted in 2008 in response to the growing "use of biometrics" in "financial transactions and security screenings."

Among its many technical requirements, the BIPA requires private entities:

- to disclose in writing to an individual what biometric identifiers or information are being collected, why they are being collected, and the length of time they will be collected or stored;
- to obtain written consent from an individual before collecting his or her biometric identifiers or information;
- to provide a publicly-available written retention policy regarding the permanent destruction of biometric identifiers or information with specific requirements;
- to destroy biometric identifiers and information within three years of an individual's last interaction with the entity, or as soon as the purpose for the collection of that person's biometric data is satisfied, whichever is earlier;
- to refrain from disclosing biometric identifiers or information except in limited circumstances;
- to refrain from selling or profiting from biometric identifiers or information; and
- to protect biometric identifiers and information in a reasonable manner that is at least as protective as the manner in which the entity protects other confidential and sensitive information.[5]

The BIPA also states that "any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party."[6] For each negligent violation of the statute, a prevailing party may recover "liquidated damages of $1,000 or actual damages, whichever is greater."[7] For each intentional or reckless violation of the statute, a prevailing party may recover "liquidated damages of $5,000 or actual damages, whichever is greater."[8] This private right of action under BIPA makes it unique among state biometrics statutes. Both Texas and Washington have biometric privacy laws as well, but neither allows for enforcement by private plaintiffs.[9] In other states, attempts to pass biometrics legislation have not passed.

In recent years, putative class action lawsuits under the BIPA have increased coincident with the growth of biometric technology tools, including fingerprinting of employees for timekeeping purposes, facial recognition for loss prevention and customer service, and biometric scans for authentication purposes in mobile applications and payment processes. Those litigation efforts have had mixed results. Some BIPA lawsuits have failed for lack of Article III standing because the plaintiff did not demonstrate an injury in fact resulting from alleged noncompliance with BIPA's requirements.[10] In contrast, a federal court in California rejected a similar argument and certified a class of Facebook users in a BIPA lawsuit challenging Facebook's allegedly non-compliant use of facial recognition technology in connection with its tag suggestions feature.[11]

Since then, dozens of BIPA lawsuits have been filed in Illinois courts often targeting employers and other entities operating physical locations in the state and allegedly capturing biometric data from individuals at those locations without satisfying all of BIPA's requirements. In fact, over 200 BIPA cases have been filed to date. The *Rosenbach* lawsuit is one such case challenging Six Flags' practice of allegedly collecting fingerprints at its parks in connection with the issuance of season passes.

The *Rosenbach* Decision

In *Rosenbach*, the plaintiff, a teenager, allegedly attended a Six Flags amusement park on a school field trip. In advance of that trip, his mother, Stacy Rosenbach, allegedly purchased a season pass for him online. She paid for the pass, but claimed that in order to complete the purchase, her son had to submit to a scan of his thumbprint when he arrived at the park. According to the pleaded allegations, Six Flags collected his biometric identifiers

and information in violation of the BIPA's disclosure, consent, and data retention and destruction requirements.

In response, Six Flags argued that the complaint should be dismissed because the plaintiff failed to plead any resulting harm from the alleged statutory violations. The intermediate appellate court agreed, finding that "a plaintiff who alleges only a technical violation of the statute without alleging some injury or adverse effect is not an aggrieved person" within the meaning of the law.[12]

In rejecting that analysis, the Illinois Supreme Court concluded that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief" under the BIPA.[13] In the court's view of statutory construction, the word "aggrieved" means suffering an infringement of a legal right without more.[14] The court also stated that a violation of the BIPA's requirements, in and of itself, is an "injury" that is "real and significant" because "when a private entity fails to adhere to the statutory procedures . . ., 'the right of the individual to maintain his or her biometric privacy vanishes into thin air.'"[15] The court did not explain, however, how an individual's privacy rights "vanish into thin air" where, for example, the plaintiff willingly provides his fingerprint to the defendant without any resulting loss or further disclosure of that data. Finally, the court stated that the "preventative and deterrent" purposes of the BIPA would not be served if plaintiffs had to suffer "some compensable injury" beyond a statutory violation before "they may seek recourse."[16]

On each of these points, there are strong countervailing considerations. For example, both federal and state courts interpreting the meaning of an "aggrieved" person in statutory schemes have found that language to require actual harm or resulting injury from an alleged statutory violation.[17] Similarly, the U.S. Supreme Court has found that the Constitution requires an injury in fact that is concrete and particularized, and more than a mere technical violation of a statute, before a plaintiff can sustain a lawsuit in federal court.[18] Moreover, with respect to statutory intent, nearly every statute can be characterized as having a preventative or deterrent purpose, but that does not mean that uninjured persons may file collective actions seeking uncapped, aggregated statutory damages that are completely untethered to any actual or compensable harm caused by purported statutory noncompliance.

Conclusion

In light of these issues, our class actions team will continue to monitor the *Rosenbach* lawsuit and advise on the latest developments in statutory standing interpretations under the BIPA. For the time being, however, the *Rosenbach* decision underscores the need for companies operating in Illinois to consider taking steps to mitigate litigation risk under the BIPA. Until the judiciary or the legislature brings some balance and consistency to the on-going wave of putative class actions under the BIPA, companies will want to consider whether biometrics-related programs make economic sense in Illinois, and if so, whether they can take preventative measures to bolster their disclosure, consent, and data protection practices, as well as their contractual terms with consumers and employees, to minimize the disproportionate risk associated with no injury, "gotcha" litigation of this sort.

Notes

1. 740 ILCS 14/1, *et seq*.
2. 740 ILCS 14/5(a).
3. *Id*. at 14/10.
4. *Id*.
5. *Id*. at 14/15.
6. *Id*. at 14/20.
7. *Id*.
8. *Id*.
9. Tex. Bus. & Com. Code § 503.001; H.B. 1493, 65th Leg., Reg. Sess. (Wash. 2017).
10. *E.g.*, Rivera v. Google, Inc., No. 1:16-cv-02714, 2018 WL 6830332 (N.D. Ill. Dec. 29, 2018).
11. In re Facebook Biometric Info. Privacy Litig., No. 3:15-cv-03747, 326 F.R.D. 535 (N.D. Cal. 2018).
12. 2017 IL App (2d) 170317, ¶ 23.
13. 2019 IL 123186, ¶ 40.
14. *Id*. ¶¶ 30–33.
15. *Id*. ¶ 34 (citation omitted).
16. *Id*. ¶ 37.
17. *See* Gubala v. Time Warner Cable, Inc., 846 F.3d 909 (7th Cir. 2017) (interpreting "aggrieved" person standard in the Cable Communications Policy Act); Spade v. Select Comfort Corp., 181 A.3d 969, 972 (N.J. 2018) (interpreting "aggrieved" consumer language in the Truth-in-Consumer Contract Warranty and Notice Act).
18. Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).