



FEBRUARY 2019

**AUTHOR**

APRIL F. DOSS

CHRISTOPHER S. NAVEJA

ERIK L. KANTZ

THOMAS LASER

## Private Lawsuit May Move Forward Over Collection of Biometric Data

### SUMMARY

On Friday, January 25, 2019, the Illinois Supreme Court sharpened the teeth of the Biometric Information Privacy Act (the “Act”). The Court ruled in favor of protecting the privacy of an individual’s biometric identifiers, holding that a plaintiff need not show any actual injury suffered in order to bring suit against companies that improperly collect or use biometric information from customers or employees. As described in our [Workplace Initiatives and Strategies for Employers \(WISE\) blog](#) this ruling raises significant challenges for companies that collect biometric information. It also adds another dimension to what has become a contested issue across the federal circuits, namely, whether the mere violation of a statutory data privacy requirement creates standing to support a private cause of action.

The Act is currently one of a kind, as very few jurisdictions recognize a private right to sue over alleged violations of data privacy protections. Under the Illinois Act, the statutory safeguards govern the collection and retention of human biometric identifiers. A “biometric identifier” includes “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.”

The Act’s purpose is to require that companies who collect biometric identifiers implement certain protections and provide certain notices governing “the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.” As stated in the Act itself:

Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

Under the Act, any person “aggrieved” by a violation the Act’s provisions “shall have a right of action . . . against an offending party” and “may recover for each violation” actual damages or liquidated damages, whichever is greater. The Act, however, fails to define what exactly constitutes an “aggrieved party.” This was the central issue in *Rosenbach*.

In *Rosenbach*, Stacy Rosenbach purchased a Six Flags season pass for her son, Alexander, in anticipation of a school field trip to Six Flags’ amusement park in Gurnee, Illinois. In order to obtain his pass, Alexander was asked to scan his thumb print into Six Flags’ biometric data capture system. Six Flags, however, did not disclose in writing how it stores and uses the biometric data, did not require that Alexander or his mother sign a release, and did not require that Alexander or his mother consent to the collection or storage of this data. In fact, the Supreme Court noted that Six Flags does not publicly disclose through a written policy what it does with this information, how it is retained, and how and when it is destroyed.



Stacy Rosenbach thereafter filed suit on behalf of her son seeking redress as an “aggrieved” person under the Act. The circuit court dismissed this claim on the grounds that Alexander had suffered no actual harm as a result of Six Flags’ conduct. The appellate court affirmed. On appeal to the Illinois Supreme Court, the central issue in the case was whether one qualifies as an “aggrieved” person and may seek damages and other relief under the Act if he or she has not alleged some adverse effect, beyond the mere violation of his or her rights under the statute. The Illinois Supreme Court answered this question in the affirmative, holding that actual injury is not required, and that any violation of the Act may give rise to a right of action. In so doing, the Court noted that “[t]o 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.”

The Supreme Court’s ruling offers guidance on what showing a plaintiff must make in order to have standing to assert a violation of its privacy rights. In fact, this issue has been the subject of a longstanding split across the federal circuits, some of which have accepted what has become the first defense in these cases: while the plaintiff’s personally identifying information may have been breached, there is no showing of actual damages or compensable harm. The Illinois Supreme Court’s ruling is especially significant in this context, as the Court expressly rejected that defense, at least as it applies to this particular state law. Now, plaintiffs have precedent to support the argument that the mere violation of a statutory requirement is enough to support not just a regulatory action, but also a private right of action. Though this ruling is only binding upon Illinois courts, it may potentially persuade other jurisdictions to adopt the same line of reasoning that the mere violation of a statutory requirement is enough to support not just regulatory action but also a private right of action.

For questions about this ruling, the Illinois Biometric Information Privacy Act, or other matters relating to data privacy and cybersecurity, please contact the authors or other members of the Saul Ewing Arnstein & Lehr Cybersecurity and Privacy practice group.

This Alert was written by April Doss, chair of the Firm’s Cybersecurity and Privacy Practice, Christopher Naveja, a partner in the Firm’s Litigation Practice, Erik Kantz, counsel, and Thomas Laser, associate. April can be reached at 410-332-8798 or [april.doss@saul.com](mailto:april.doss@saul.com). Christopher can be reached at 312-876-7140 or [christopher.naveja@saul.com](mailto:christopher.naveja@saul.com). Erik can be reached at 312-876-6671 or [erik.kantz@saul.com](mailto:erik.kantz@saul.com). Thomas can be reached at 312-876-7161 or [tom.laser@saul.com](mailto:tom.laser@saul.com). This publication has been prepared for information purposes only.

The provision and receipt of the information in this publication (a) should not be considered legal advice, (b) does not create a lawyer-client relationship, and (c) should not be acted on without seeking professional counsel who have been informed of the specific facts. Under the rules of certain jurisdictions, this communication may constitute “Attorney Advertising.”