Illinois Supreme Court Ruling: Biometric Privacy Law Only Requires Violation, Not Actual Harm

Insights
2.06.19

Summary

On January 25, 2019, the Illinois State Supreme Court ruled that the state's Biometric Information Privacy Act (BIPA) only requires individuals to show violation of the law to bring suit. Businesses with a presence in Illinois that gather "biometric identifiers", which include a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, are now at a greater risk of liability if they do not follow legally required procedures for such data collected or stored in the state. BIPA's applicability at the federal level remains to be seen, but similar laws are being considered throughout the states, raising potential liability for employers elsewhere.

Background

The Biometric Information Privacy Act was passed by Illinois lawmakers in 2008 and stipulates that a company doing business in the state must obtain written consent from an individual before collecting their biometric identifiers In addition, companies must also disclose their policies for use and retention of the biometric data. Violations of BIPA incur a $1,000 fine per infraction, and $5,000 per infraction if one is found to be intentionally or recklessly violating the Act.

Though Illinois was the first state to pass a law specifically regulating biometric data usage, Washington and Texas have already passed similar legislation, with more states considering the issue and others expanding protections already in place. For now though, BIPA is the only state law allowing private suit and recovery of damages for violations.

In the class action at issue, Rosenbach v. Six Flags Entertain. Corp., plaintiff Stacy Rosenbach purchased a season pass for her 14 year old son as part of a school field trip to Six Flags Amusement Park. Upon arrival at the park, her son was required to submit to a fingerprint scan in order to use the pass. At no point before her son attempted to activate the pass was Rosenbach informed about the fingerprinting requirement or how the information would be used or stored. Importantly, Rosenbach did not claim that the violation caused financial or other harm. Upon reviewing these facts, The Illinois Supreme Court accepted her argument that the Six Flags policy violated the act, and that the violation of BIPA alone was sufficient to bring suit. Specifically, the court stated that an "aggrieved" person "may seek liquidated damages and injunctive relief pursuant to

the Act even if he or she has not alleged some actual injury or adverse effect, beyond violation of his or her rights under the statute."

Applicability Limited...For Now

Though the Rosenbach ruling clarifies who is allowed to bring suit for violations of BIPA, the issue of which types of injuries are sufficient to provide standing in federal court remains unclear, with district courts across the country coming to different conclusions on what constitutes a "concrete" injury. The most recent ruling come in a December 29, 2018 Northern District of Illinois decision which held that neither the collection nor retention of templates from Google Photos' "face grouping" feature [1] a facial recognition system which automatically scans photos to create individualized face templates - presented a "concrete" injury. This ruling pivoted on the lack of evidence that Google's practices created a substantial risk of harm because Google had not leaked or disclosed the information to third parties. The court emphasized this would be the case even if users did not know Google was obtaining biometric data.

In two similar cases brought against Facebook for its use of "faceprint" technology in the Northern District of California, the court declined to dismiss the plaintiff's claims under BIPA, relying on the Illinois legislature's interpretation that since biometric data cannot be changed, it presents a heightened risk of identity theft.

These conflicting outcomes illustrate the approaches courts are using to address the potential privacy-based harms that grow out of current technology, with some courts deferring to legislative interpretations, while others require a more traditional tort analysis.

Wrapping Up

Under Illinois law, businesses now face potential liability for failing to properly follow procedures for handling biometric information, regardless of whether the claimant suffered "actual" harm. As a result, entities using these technologies face a higher risk of litigation. Already, a nationwide fashion retailer is facing a class action by former and current employees for violations of BIPA due to its biometric punch clock policies, while a fast food chain faces a similar suit. At present, the issue of standing at the federal level remains unresolved, but employers would be well advised to adopt procedures similar to those required under BIPA, as more states are considering or have already introduced similar legislation, and others have expanded expectations for employers to protect employees' biometric data.

Related People

Robert Fallah
Attorney
610.230.2150
Email