BARNES & THORNBURG LLP

ARTICLES

No Harm, No Foul? Not So Fast: The Illinois Supreme Court Allows BIPA Lawsuits Without Allegations Of Actual Injury

June 5, 2019

What is BIPA?

The Illinois legislature enacted the BIPA in 2008 in order to protect citizens' biometric information from falling into the wrong hands. Unlike other sensitive data (like Social Security numbers), biometric information cannot be changed if it is compromised. The BIPA regulates private entities' collection and storage of "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." Biometric information includes "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." Private entities are forbidden from collecting or storing biometric information unless certain requirements are met.

Although a handful of states have enacted or proposed similar biometric information privacy laws (such as Connecticut, Montana, New Hampshire, Texas, and Washington) Illinois' law is unique in that it allows for a private right of action. The BIPA provides for a minimum of $1,000 or actual damages, whichever is greater, per violation (i.e. per fingerprint), and even more, along with attorneys' costs and fees, if the violation is intentional or a result of reckless conduct.

The *Rosenbach* Decision

In *Rosenbach v. Six Flags Entertainment Corporation*, 2019 IL 123186, the plaintiff sued Six Flags Entertainment Corporation under the BIPA after Six Flags scanned her son's fingerprint without obtaining written

RELATED PEOPLE

Christine E. Skoczylas
Partner
Chicago

P 312-214-5613
F 312-759-5646
christine.skoczylas@btlaw.com

Dana Amato Sarros
Associate
Chicago

P 312-338-5921
F 312-759-5646
dana.amato@btlaw.com

RELATED PRACTICE AREAS

Commercial Litigation

consent and without properly disclosing the company's business practices relating to the collection, use, and retention of the fingerprint data. Six Flags filed a motion to dismiss on the grounds that the plaintiff was not an "aggrieved party" under the statute because she had not alleged any "actual injury." This motion was denied, but Six Flags successfully filed a motion for reconsideration. Six Flags won at the appellate level before the case landed in the Illinois Supreme Court.

The central question before the Supreme Court was whether a party is "aggrieved" under the BIPA if she only suffered a violation of the notice and consent requirements without sustaining actual injury. The Supreme Court found that such an individual *does* have standing to sue.

According to the "principles of statutory construction," the Supreme Court found that a person need not have sustained actual damage, beyond violation of her rights under the BIPA, in order to bring suit. Because the term "aggrieved" is not defined in the statute, the court relied on the word's "settled legal meaning," as established more than a century ago –namely, that "a person is prejudiced or aggrieved in the legal sense, when a legal right is invaded by the act complained of or his pecuniary interest is directly affected by the decree or judgment."

The court also noted the Illinois legislature's concern that biometrics are unlike other unique identifiers because an individual has no recourse once her biologically unique information has been compromised. Therefore, the court reasoned, forcing a plaintiff to wait until she has sustained this type of injury before seeking recourse would be "completely antithetical to the Act's preventive and deterrent purposes."

Where Do We Go From Here?

Predictably, BIPA lawsuits have flourished in the wake of *Rosenbach*. Tech giants like Facebook, Google, and Snapchat have all been sued under Illinois' BIPA. In the past two years, more than 200 class actions have been filed in Illinois, and that number will likely continue to rise.

Illinois business should take care to follow best practices for collecting and storing biometric information, including creating a written policy that establishes guidelines and a schedule for permanently destroying biometric data that had been collected; receiving acknowledgement and release from individuals before collection or storage; and refraining from disclosing the data, whether by accident (i.e., hacking) or by selling, leasing, trading, or otherwise profiting from it. The best advice is to read the statute, understand its provisions, obtain appropriate advice, and make adjustments to practices and policies in order to comply with its requirements. If you determine that your company is collecting and storing biometrics, you should immediately evaluate your current practices from legal compliance and potential exposure standpoints.