

# CLIENT ALERT

January 29, 2019

1

## DATA PRIVACY AND CYBERSECURITY

### **WITH EVERYONE BEING THE VICTIM OF A DATA BREACH, THE ILLINOIS SUPREME COURT'S DECISION NOT REQUIRING ACTUAL HARM TO PURSUE A CLAIM FOR IMPROPER COLLECTION OF BIOMETRIC DATA MAY GIVE A HINT OF THE FUTURE**

by Sara H. Jodka

There are three states with biometric privacy laws. Texas, which passed its law in 2009, and Washington, which passed its law in 2017, followed Illinois' passage of its 2008 law, the Biometric Information Privacy Act (BIPA) which remains the most stringent in the country. The Illinois law has been the focus of a number of class action lawsuits, including suits against Facebook and Google. On January 25, 2019, the Illinois Supreme Court levied a decision against Six Flags that will have significant consequences on any entity collecting biometric data in Illinois.

By way of background, BIPA provides that companies doing business in Illinois must obtain express written consent from an individual *before* they can collect biometric data, which includes fingerprints, retinal scans, facial recognition data points, etc. The law provides for a private right of action and has monetary penalties set at \$1,000 per violation, and \$5,000 per violation *if* the entity violates the law intentionally or recklessly.

The case at issue concerned Six Flags' practice of collecting and storing guests' fingerprints. Stacy Rosenbach sued on behalf of her son claiming that Six Flags fingerprinted her 14-year-old son when he picked up a season pass and stored his fingerprints without the required express written consent.

In response, Six Flags argued that Rosenbach was not an "aggrieved person" to qualify for damages under the statute because she had to – but could not – demonstrate that the collection of her son's fingerprint data resulted in actual harm.

The appellate court held that a technical violation of BIPA standing alone and without any actual harm was not a recoverable violation under the law.

The Illinois Supreme Court reversed and, in doing so, first addressed its attention to the purpose of the statute, which it felt was not properly considered by the appellate court's holding. Specifically, high court noted that BIPA vests individuals and customers with the right to control their biometric information by requiring express written notice before such information is collected, thereby, giving them the power to object to the collection and have more control over it. The issue the Supreme Court noted was that, without any teeth to it, *i.e.*, by requiring that someone suffer actual harm before they can sue for improper collection, any private entity could just subvert the consent requirement and render meaningless the consumer rights granted under the law.

The Illinois Supreme Court then went on to discuss the significance of the private right of action component in the law, which is significant because, unlike breach statutes that allow the state attorney generals to bring suit against offending companies, there is no such allowance in BIPA. As such, the Court held the individual private right of action component was clearly intended to have significant application.

Combining these two points, the Court overruled the appellate court allowing redress under BIPA for technical violations and not requiring prove of actual injury or damage beyond infringement of the rights afforded under the law.

#### Takeaways

For those entities doing business and, more specifically, collecting biometric data in Illinois, the holding is significant. It is a victory for consumers as it ensures them clear rights to their biometric information, in Illinois at least. As for those entities, including tech giants Facebook and Google, the decision will, no doubt, have serious impact on the class actions currently filed against them and their standard operating procedures for collecting biometric data in Illinois.

The Illinois Supreme Court's decision finding that actual harm is not necessary for a claim is significant, especially in data collection cases because providing actual harm for collected, improperly disseminated, breached, etc., data is extremely difficult. This is especially true when it would seem that everyone has been the victim of a breach in one way or another and, as a result, their personal information spread all over with no real way to prove actual damage.

While Illinois is the only law to include a private right of action, more may come along. If they follow the Illinois Supreme Court's holding in *Rosenbach v. Six Flags*, they will impose statutory penalties with a private right of action which does not require actual harm, which is extremely hard to demonstrate in data collection cases.

*This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of Data Privacy and Cybersecurity. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.*

FOR MORE INFORMATION CONTACT:



**Sara H. Jodka**, CIPP-US is a Member in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or [sjodka@dickinsonwright.com](mailto:sjodka@dickinsonwright.com).