

January 28, 2019

Illinois Supreme Court Holds that the Illinois Biometric Information Privacy Act is a Very Expensive Trap for the Unwary

By Justin O. Kay

On January 25, 2019, the Illinois Supreme Court issued its much-anticipated decision in *Rosenbach v. Six Flags Entertainment Corporation* interpreting the meaning of the term “aggrieved” in the Illinois Biometric Information Privacy Act (BIPA). Specifically, the court was asked to address whether to be “aggrieved” (a prerequisite to filing a suit for \$1,000 - \$5,000 in statutory damages per violation) a private plaintiff need merely allege that defendant violated the statute’s technical requirements regarding the collection, use, and storage of biometric information, or whether a plaintiff must also allege some actual harm arising from that technical violation.

Invoking its interpretation of other statutes, the dictionary definition of the term “aggrieved,” and consumer privacy policy considerations, the Illinois Supreme Court ruled that the failure to comply with BIPA’s technical requirements alone is sufficient to state a claim, and that “no additional consequences need be pleaded or proved.”

This decision’s establishment of such a low bar for filing suit will have a significant impact on the many BIPA lawsuits already pending, spur additional BIPA lawsuits, and generate further discussions regarding amending the statute following two failed efforts in recent years to do so. It will also influence ongoing efforts in other states to enact biometrics-related legislation and impact broader discussions regarding the enactment of comprehensive federal privacy regulations. And it will likely have a chilling effect on the use of biometric technology in Illinois.

What is BIPA?

BIPA regulates the collection, use, and storage of “biometric identifiers” and “biometric information,” defined respectively as “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry” (with narrow exclusions for such things as samples used for medical or scientific purposes) and “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.”

BIPA includes a number of technical requirements regulating the collection, use, and storage of biometric identifiers and biometric information. **First**, it prohibits

the collection of biometric identifiers or information without obtaining a signed, written release informing the person of the collection, the specific purpose for collection, and the length of time the identifiers or information will be retained. **Second**, it forbids the sale, lease, or profit from the identifiers or the information and prohibits disclosure of them except in narrow circumstances (such as with the person’s consent). **Third**, it requires anyone in possession of such identifiers or information to safeguard them using the reasonable standard of care for the industry, and requires protections to be put in place that are at least “the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.” **Fourth**, it requires anyone in possession of identifiers or information to develop and adhere to a publicly available written policy establishing a retention and destruction schedule under which the identifiers or information will be retained for no longer than the earlier of when the original purpose for their collection is satisfied, or three years.

What Happened in *Rosenbach*?

Rosenbach reached the Illinois Supreme Court as a pair of certified questions asking whether an individual is aggrieved where the only injury alleged is that a person was not provided with the required disclosures and that the identifiers or information were collected without obtaining the written release. The person in *Rosenbach* was a 14-year-old boy who, in order to obtain a season pass to visit an amusement park in Illinois, provided a thumb-scan that was used to verify his identity when he patronized the park. He was not provided with the written disclosures described above and did not execute a release. He filed a purported class action lawsuit two years later based on the lack of the disclosures and release, but did not allege any adverse consequences arising from not receiving them, and did not allege that his thumb-scan data had been shared, compromised, or misused.

The defendant moved to dismiss, arguing that the plaintiff was not “aggrieved” because there were no allegations of actual injury. The trial court disagreed and denied the motion, but eventually agreed to certify the issue to the appellate court. The appellate court, however, sided with the defendant, finding in

a December 2017 opinion that an “aggrieved” person must allege some “actual harm.” According to the appellate court, “if the Illinois legislature intended to allow for a private cause of action for every technical violation of the Act, it could have omitted the word ‘aggrieved’ and stated that every violation was actionable. A determination that a technical violation of the statute is actionable would render the word ‘aggrieved’ superfluous.”

The Illinois Supreme Court granted the plaintiff’s petition for certiorari in May 2018; heard oral argument in November 2018 (which, in a departure from usual practice, it broadcast live); and on January 25, 2019, issued a unanimous opinion reversing the appellate court’s decision.

As noted above, the Illinois Supreme Court started by comparing and contrasting the language used in other acts and determined that BIPA follows the model employed by the AIDS Confidentiality Act, which does not require proof of actual damages to recover. The court found support for this interpretation in the “standard definitions” of “aggrieved” found in dictionaries. The court found further support in BIPA’s preamble, reasoning that the public policy considerations identified therein (e.g., that things like one’s face and fingerprints cannot be changed if compromised) demonstrated that the legislature intended to (i) impose safeguards to ensure that consumer privacy rights and preferences are honored and protected, and (ii) subject private entities who fail to follow those safeguards to “substantial potential liability.” In the court’s view, the risk of ruinous liability for a technical violation was actually a positive because “entities have the strongest possible incentive to conform to the law and prevent problems before they occur and cannot be undone,” and, in any event, “[c]ompliance should be easy.”

What Happens Now?

The Illinois Supreme Court’s decision in *Rosenbach* creates a very expensive trap for those who use biometrics for any purpose without careful review of the program beforehand. Any company doing business in Illinois should conduct a rapid internal audit to determine whether it or any agent or contractor is using or exploring the use of biometrics for any reason (e.g., security for facilities or devices, convenience for consumers or employees, marketing to consumers). If so, that audit should be followed by verification that either in-house or outside counsel was involved in the program and approved its implementation.

What Happens Next?

In 2008, Illinois was the first state to pass a law regulating the collection, use, and storage of biometric information, and that law (BIPA) remains the most onerous and only one with a private right of action. The *Rosenbach* decision makes BIPA even more onerous, and any relief will likely need to come from the Illinois legislature. But efforts to amend the law have not succeeded: in response to the recent spate of lawsuits, legislators have twice introduced (most recently in February of last year) amendments designed to limit the scope of BIPA, but neither proposal advanced.

Many other states have considered biometric privacy legislation over the years, but only Texas (in 2009) and the state of Washington (in 2017) have passed such laws. But that looks to change soon. The rate at which state legislators are introducing these bills has accelerated over the past couple of years as the use of the technology has become more commonplace: in the first few weeks of 2019 alone, legislators have already introduced new bills in Arizona, Connecticut, New Hampshire, New Mexico, New York, Oregon, and Washington. These initiatives have the potential to introduce a conflicting national patchwork of regulations that might only be resolved through comprehensive federal legislation.

Litigation Group

Primary Contacts



Justin O. Kay

Partner

Chicago
(312) 569-1381

justin.kay@dbr.com

Drinker Biddle

www.drinkerbiddle.com

CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY | NEW YORK | PENNSYLVANIA | TEXAS | WASHINGTON DC | LONDON

© 2019 Drinker Biddle & Reath LLP. All rights reserved. A Delaware limited liability partnership. Promotional Materials 2019. One Logan Square, Ste. 2000, Philadelphia, PA 19103-6996 (215) 988-2700 office (215) 988-2757 fax
Jonathan I. Epstein and Andrew B. Joseph, Partners in Charge of the Princeton and Florham Park, N.J., offices, respectively.