ROPES & GRAY

ALERT

Privacy & Cybersecurity

January 8, 2018

Private Rights of Action under Illinois Biometric Privacy Statute Sharply Limited

Attorneys
Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Seth C. Harrington
Mark P. Szpak
Michelle Visser
David T. Cohen
Kevin J. Angle
Deborah L. Gersh

On December 21, 2017, a three-judge panel of the Second District Appellate Court of Illinois significantly narrowed the ability of plaintiffs to bring a private right of action under Illinois' Biometric Information Privacy Act ("BIPA" or "Act"). BIPA provides for a private right of action and liquidated damages of $1,000 per violation (or $5,000 for intentional or reckless violations) to persons "aggrieved by a violation" of its restrictions on the collection, use and sharing of certain biometric data, and class actions under the statute have recently proliferated. Answering questions certified by the trial court below, the intermediate appellate court in *Rosenbach v. Six Flags & Great America*, 2017 IL App (2d) 170317, held that BIPA requires plaintiffs to "allege some actual harm" instead of merely showing that defendants failed to comply with the statutory requirements.

Background

BIPA regulates how certain private entities handle customers' biometric information, which the Act defines as identifying information based on "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." The Act prohibits certain use of biometric information, and it requires those who possess biometric information to adopt certain retention and destruction policies. It also mandates that any entity that collects biometric information must supply written notices to the subject about the collection of the information and the purpose for doing so. BIPA provides for a private right of action and liquidated damages of $1,000 per violation (or $5,000 for intentional or reckless violations) to persons "aggrieved by a violation" of these requirements.

BIPA has given rise to an outbreak of high-stakes lawsuits over the last few years. Facebook continues to defend a putative class action suit in a California federal court for using facial recognition software on photos that users upload to the site. Last November, United Airlines and McDonalds were both served Illinois court class-action complaints under the Act, in which employees claim that the fingerprint-based timekeeping and employee-tracking systems collect their biometric data without adhering to BIPA's notice and consent requirements. These and other pending cases pose significant potential liability to the defendants.

BIPA class action defendants have seen mixed results when seeking dismissal of the suits they face. Of particular importance, federal district courts have reached conflicting conclusions as to whether a plaintiff must plead and prove actual adverse consequences from the alleged statutory violation in order to pursue his or her claims.

Rosenbach v. Six Flags

The *Six Flags* decision provides important guidance on whether actual injury is required by BIPA by limiting the class of persons "aggrieved by a violation" to those who suffer "actual harm or adverse consequences," rather than "a mere technical violation of the statute." When the plaintiff's son purchased a Six Flags season pass, the park allegedly collected his fingerprints for security purposes without obtaining consent or providing the required disclosures.

The court looked to plain meaning and case law from other jurisdictions to determine whether actual injury is required to qualify as an "aggrieved" person under the statute. The court first drew from dictionary definitions to find

that a plaintiff must generally show "an actual injury, adverse effect, or harm" in addition to an infringement of legal rights to be "aggrieved" by a statutory violation. Additionally, the opinion said, if the legislature had intended to provide a cause of action for every violation of the statute, it could have said so explicitly instead of qualifying the persons eligible to sue with the word "aggrieved." The court then considered, among other things, federal district court opinions from the Northern District of Illinois and the Southern District of New York that found allegations of mere technical violations of BIPA's notice and consent requirements insufficient to meet the standard of "aggrieved party." The court concluded that a remedy under the Act was not available without an actual injury or adverse effect beyond a technical violation. It qualified this holding, however, by noting that "the adverse injury or adverse effect need not be pecuniary."

Implications

Six Flags supplies a powerful tool for defendants to obtain dismissal of BIPA claims. Companies may often have arguments that their mere collection or other handling of biometric data caused no injury to plaintiff at all, requiring dismissal. Further, the ruling will likely make it harder for plaintiffs to obtain class certification under BIPA.

Though this decision solidifies a reading of the Act that favors defendants, there are still important limitations. First, as noted above, the court explicitly qualified its holding by stating that the injury or adverse effect "need not be pecuniary." Additionally, while federal courts will likely give significant weight to this intermediate appellate court's interpretation of BIPA, the Illinois Supreme Court has not yet spoken on the matter.

Actions under BIPA and similar statutes continue to threaten companies with especially significant liability given their potential to implicate large classes of plaintiffs. Internet of Things devices, for example, increasingly use biometric identifiers such as fingerprints, facial scans, or voice data to identify users or provide other services. Given the proliferation of such devices, even minor transgressions of BIPA can amount to numerous alleged violations. At $1,000 to $5,000 per claim in liquidated damages, the risk to companies remains substantial.

For more information regarding BIPA, or to discuss privacy or cybersecurity practices generally, please feel free to contact Heather Sussman, Doug Meal, Jim DeGraw, Seth Harrington, Mark Szpak, Michelle Visser, David Cohen, Kevin Angle, Debbie Gersh, or another member of Ropes & Gray's leading privacy & cybersecurity team.