BARNES & THORNBURG LLP

Illinois Supreme Court BIPA Ruling Triggers Risks For Private Employers

February 1, 2019 | Social Media And Technology,Labor And Employment

The Illinois Supreme Court ruled on Jan. 25 that a company's technical violation of the Biometric Information Privacy Act (BIPA) gives an individual standing to file a lawsuit. The court found that a technical violation amounts to substantial harm, which creates liabilities for Illinois employers that rely on employee fingerprints for electronic time-keeping, and opening the door to potential class actions.

BIPA, in effect since 2008, prohibits businesses from collecting and disseminating biometric information without an individual's prior informed written consent. BIPA also provides that any person "aggrieved" by a violation of the act's provisions may sue and "recover for each violation" the greater of liquidated damages or actual damages, and reasonable attorney fees.

The Illinois Supreme Court recent decision in *Rosenbach v. Six Flags Entertainment Corp* carries serious implications for private businesses that collect biometric information, such as fingerprints, from customers and employees. In *Rosenbach*, the lawsuit involved a young customer of the Six Flags theme park in Gurnee, Illinois, who had given his fingerprint as part of buying a season pass to the theme park. (Six Flags began collecting fingerprints from season pass holders in 2014 and used that information to verify customer identities, streamline admission, and combat fraud.)

But, Six Flags' young customer was not told before buying his season pass why Six Flags needed his fingerprint or how long the information would be kept. There was no written permission, consent, or release. His family filed suit against Six Flags for the technical violations.

Six Flags defended itself by arguing the lack of actual harm. The central issue in the lawsuit was whether a "technical violation" of BIPA alone, without a showing of an actual injury, is enough of a foundation to bring a lawsuit.

RELATED PRACTICE AREAS

Data Security and Privacy
Labor and Employment

RELATED TOPICS

security
Recordkeeping
data

On Friday, the Illinois Supreme Court held that plaintiff could sue under BIPA, because the consequences of compromised biometric information are “real and significant” in today’s digital era. The Illinois high court explained that BIPA’s procedural protections “are particularly crucial in our digital world because technology now permits the wholesale collection and storage of an individual's unique biometric identifiers that cannot be changed if compromised or misused.” Therefore, when a private entity fails to adhere to the statutory procedures, “the right of the individual to maintain his or her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized. This is no mere technicality. The injury is real and significant.”

This decision appears in conflict with the U.S. Supreme Court’s 2016 decision in *Spokeo, Inc. v. Robins,* where SCOTUS determined that a technical violation alone is not enough to sue. In *Spokeo*, a plaintiff sued an online white pages company for posting inaccurate information about him in violation of the Fair Credit Reporting Act. The plaintiff could not show how false information about him, such as his marital status and age, materialized in the real world and injured his reputation or employment prospects. The Supreme Court held a plaintiff must demonstrate that his or her injury is both concrete and particularized, and this injury-in-fact requirement is a constitutional requirement that Congress could not erase by enacting a statute.

The Illinois Supreme Court’s decision should be viewed in the limited context of lawsuits arising out of the Biometric Information Privacy Act. The court’s main concern is that biometric information, such as fingerprints and retina scans, are immutable, and what may be a “technical violation” is not a “mere technicality.” By contrast, consumer information in *Spokeo* involved social security numbers and online postings, which could be changed and corrected.

Illinois employers who ask employees to provide fingerprints or other biometric information as part of their internal security would be wise to pay attention to this case, and to the rules of complying with BIPA.