

Services

Data Privacy &
Cybersecurity

Labor & Employment
State Privacy Laws

Professionals

ANNE M. MAYETTE

CHICAGO:

312.341.9844

ANNE.MAYETTE@

HUSCHBLACKWELL.COM

TERRY L. POTTER

ST. LOUIS:

314.345.6438

TERRY.POTTER@

HUSCHBLACKWELL.COM

No Actual Damages Required to Protect Privacy Rights Under Illinois Biometric Information Privacy Act

On January 25, 2019, the Illinois Supreme Court released a unanimous decision holding that individuals do not need to plead or prove actual damages or harm to maintain a private right of action under the Illinois Biometric Information Privacy Act (740 ILCS 14/1) (the Act) when a private entity fails to comply with the Act's procedural protections. The decision upholds privacy rights of individuals in their unique biological information as defined under the Act.

The Facts

Six Flags Entertainment Corporation (Six Flags) scans thumbprints as part of their season pass holder system and stores the biometric information in their biometric data capture system. In 2014, prior to scanning the fingerprints of prospective season pass holders, Six Flags failed to: 1) disclose the collection of the biometric information, 2) disclose the purpose or period of time for which it stored the information, and 3) obtain a written release regarding the scan of the thumbprint. Stacy Rosenbach, the mother of a 14-year-old boy whose thumbprint was scanned, sued Six Flags for violation of the procedural protections under §15(b) of the Act on behalf of her minor son and all similarly situated individuals.

Defendants filed a motion to dismiss arguing that an “aggrieved” person under the Act is limited to individuals who suffer actual damages or harm and requires more than “a technical violation” of the Act. Through a series of appeals, the 2nd District Illinois Appellate Court agreed with defendants and granted their motion to dismiss. The holding by the Court of Appeals resulted in a split among the appellate courts regarding whether actual damages were

required under the Act. The Illinois Supreme Court granted an appeal and de novo review.

Illinois Biometric Information Privacy Act

The Act defines biometric information as biometric identifiers, regardless of how they are captured, converted, stored or shared, that are used to identify an individual. Biometric identifiers refer to retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry.

Section 15(b) of the Act imposes certain procedural obligations, relating to disclosure and consent, on private entities that collect, capture or store the biometric information of an individual to:

Disclose that biometric information is being collected or stored;

Disclose in writing the purpose and the length of time for which the biometric information is being collected, stored and used;

Obtain a written release documenting consent to the collection, storage and use of the biometric information.

Section 20 of the Act provides a private right of action to “aggrieved” persons to enforce the obligations placed on private entities as follows:

“Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or ... against an offending party. A prevailing party may recover for each violation...”

The Illinois Supreme Court Decision

The term “aggrieved” is not defined in the Act. The Court reviewed Illinois case law and other Illinois statutes, such as the AIDS Confidentiality Act, to establish that an “aggrieved” person refers to an individual denied some personal or property right. Violation of that legal right does not require that the individual sustain monetary or pecuniary damages to qualify as “aggrieved.” The established meaning of the term “aggrieved” together with the provisions of §5 of the Act convinced the Court that violation of the Act did not require actual damages.

Section 5 of the Act codifies the Illinois legislature intent to adopt procedural protections to safeguard a person’s right to privacy and control over their unique biometric information and identifiers. The legislature recognized that once biometric information is compromised, an individual has no recourse, and that the full consequences of losing control over biometric information are incapable of ascertainment. As such, regulation of collection, use, protection, handling, storage, retention and destruction of biometric identifiers and information safeguards public safety, welfare and security.

Based on the plain language of the statute, the Court held that a person is not required to plead or prove actual damages when a private entity fails to fulfill their obligations under §15(b) of the Act. In reaching its holding, the Court recognized that the potential compromise of a person's biometric information is "no mere technicality" but "real and significant." It described compliance with procedural protections required by the Act as "crucial" to safeguarding unique biometric information and a person's right to maintain their biometric privacy.

What This Means to You

Businesses operating in Illinois that collect or possess biometric identifiers or biometric information must develop a written policy available to the public and a retention and destruction schedule for permanently destroying the biometric information. In addition, *prior to* collection of the biometric information, businesses must disclose their intent to collect the information; provide written documentation of the purpose and length of time for which the information is collected, stored and used; and receive a written release.

The Act also regulates dissemination, storage and transmittal of biometric information. Selling, leasing, trading or otherwise profiting from a person's biometric information is strictly prohibited.

Contact Us

If you have questions about the Illinois Biometric Information Privacy Act, concerns about compliance with the Act or implications of the Court's decision, contact Anne Mayette, Terry Potter or your Husch Blackwell attorney.

Tracey Oakes O'Brien was a contributing author of this content.