masuda funai

News & Types: Employment, Labor & Benefits Update

Illinois Supreme Court Issues Ruling in Landmark Biometric Information Privacy Case

2/5/2019

By: Kenton P. Knop

Practices: Employment, Labor & Benefits, Intellectual Property & Technology, Litigation

EXECUTIVE SUMMARY

The Illinois Supreme Court's recent ruling that actual harm is not required to establish a cause of action for a violation of Illinois's Biometric Information Privacy Act ("BIPA") affirmed BIPA's "preventative and deterrent" purposes. Businesses that anticipate coming into contact with biometric identifiers or biometric information of Illinois residents should conduct an immediate review of their biometric data collection and handling policies and practices, and take appropriate action to ensure that they are in full compliance with BIPA's requirements.

On January 25, 2019, the Illinois Supreme Court issued its ruling in the *Rosenbach v. Six Flags Entertainment Corp.* case (2019 IL 123186), decisively stating that a plaintiff is not required to suffer actual harm to have a cause of action for a violation of Illinois's Biometric Information Privacy Act (740 ILCS 14/1 *et seq*.) ("BIPA"). The Court's ruling resolves the recent conflict among Illinois courts, which had disagreed on whether a "technical violation" of BIPA's requirements without actual harm could give a plaintiff the ability to sue a non-compliant business as an "aggrieved" party. BIPA is the only biometric information privacy law in the United States to provide for a private cause of action, and provides for actual damages or statutory liquidated damages ($1,000 for each negligent violation or $5,000 for each intentional or reckless violation), reasonable attorneys' fees and costs, and the availability of injunctive relief for prevailing plaintiffs. 740 ILCS 14/20.

The main consequence of this ruling is that businesses and other "private entities" that contemplate utilizing biometric identifiers and biometric information of employees or customers located in Illinois, such as fingerprint scanning for employee timekeeping or "season pass" customer verification purposes, must ensure strict compliance with BIPA's requirements or risk significant penalties, potentially in the form of a class action lawsuit. Under BIPA, "biometric identifiers" are an individual's retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, and "biometric information" means any information based on an individual's biometric identifier that is used to identify an individual. 740 ILCS 14/10. To ensure compliance with BIPA, businesses must first take the following steps:

1. Develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers/information. Biometric identifiers/information must be destroyed when the initial purpose for collecting or obtaining the identifiers/information has been satisfied, or within 3 years of the individual's last interaction with the private entity, whichever occurs first. 740 ILCS 14/15(a).
2. Before collecting or obtaining an individual's biometric identifier/information, a private entity must perform the following:
    a. Inform the subject individual in writing that a biometric identifier/information is being collected or stored;
    b. Inform the subject individual in writing of the specific purpose and length of term for which a biometric identifier/information is being collected, stored, and used; and
    c. Receive a written release executed by the individual who is the subject of the biometric identifier/information. 740 ILCS 14/15(b).

A business's responsibilities under BIPA continue after it has collected the biometric identifier/information. A private entity may not sell, lease, trade or otherwise profit from a person's biometric identifier/information. 740 ILCS 14/15(c). In addition, a private entity may not disclose an individual's biometric identifier/information except in limited circumstances, such as with the prior consent of the subject individual, to complete a financial transaction requested or authorized by the subject individual, or as required by applicable law or pursuant to a valid warrant or subpoena. 740 ILCS 14/15(d). Finally, a private entity must store, transmit, and protect from disclosure all biometric identifiers/information using the reasonable standard of care within the private entity's industry, and in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects its other confidential and sensitive information. 740 ILCS 14/15(e).

As companies continue to adopt new technologies utilizing biometric information to streamline identification of their employees and provide personalized services to customers, compliance with state biometric information protection statutes such as BIPA will become increasingly important. In light of the Illinois Supreme Court's affirmation of BIPA's "preventative and deterrent" purposes, businesses that anticipate coming into any type of contact with biometric identifiers or biometric information of Illinois residents should conduct an immediate review of their biometric data collection and handling policies and practices, and take appropriate action to ensure that they are in full compliance with BIPA's requirements. If there are any questions of previous non-compliance under BIPA, we recommend contacting legal counsel as soon as possible.