akerman

Practice Update

Florida Employers Using Biometric Time-Keeping May Face New Risks

March 7, 2019

By John T. Roache, Mark S. Bernstein, and Thomas Y. Mandler

The Florida legislature is considering a bill regulating the biometric data employers collect from their workforces. The new bill mirrors the Illinois Biometric Information Privacy Act (BIPA), which has led to hundreds of class actions filed in Illinois courts by workers against their employers over alleged violations. Based on the Illinois Supreme Court's recent interpretation of BIPA, that trend does not appear to have an end in sight. For Florida employers, BIPA and those cases have taken on a new importance as the Florida Senate considers going down the same road. Now is the time for Florida employers to review their policies and procedures to ensure they comply with BIPA requirements.

Many employers concerned about facility security or maintaining the integrity of employee time records utilize finger scans and other scanning technology to track the access to and presence of employees in their facilities. In most circumstances, the employer or its vendor does not store actual fingerprints, but instead stores a unique numeric algorithm. Although the new technology has significant business benefits, it also creates risks. Three states, Illinois, Texas, and Washington, have enacted laws to address the commercial use of biometric information obtained from individuals. Illinois, unlike Texas or Washington, allows for a private right of action, and

Related People

Mark S. Bernstein
Thomas Y. Mandler
John T. Roache

Related Work

Labor and Employment

Related Offices

Chicago

the available relief includes actual and statutory damages, injunctive relief and attorneys' fees. Those potential remedies have resulted in an onslaught of class actions against employers under BIPA.

If enacted by the Florida legislature, the Florida law will create a breeding ground for class action lawsuits against Florida employers using biometric scanning technology. Accordingly, Florida employers should be aware of and comply with the BIPA requirements to the extent that they are utilizing biometric scanning technology. Given the conservative makeup of the Florida legislature, it seems unlikely that the current bill was pass. Nevertheless, Florida employers looking to meet best practices should implement procedures and policies to comply with BIPA requirements.

Illinois defines biometric information means any information, regardless of how it is captured, converted, stored or shared, based on an individual's biometric identifier which includes a retina or iris scan, fingerprint, voiceprint, or a hand or face scan used to identify an individual. Illinois places the following obligations on employers' collection, use and storage of employee biometric information. Employers may collect and use employee biometric information if they:

1. Provide notice to employees that their information will be collected, used, and stored;
2. Obtain employee consent in writing for the collection, use, and storage of biometric information; and
3. Take precautions to prevent the unauthorized use or disclosure of that biometric information, including destruction after the information will no longer be used.

An employer also must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric information when the initial purpose for

collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with the private entity, whichever occurs first.

BIPA also prohibits employers from:

1. Selling, leasing, trading, or otherwise profiting from an employee's biometric information; or
2. Disclosing, redisclosing, or otherwise disseminating an employee's biometric information unless it qualifies for one of the enumerated exceptions.

It is critical that Florida employers:

1. Obtain written consent from employees who are using biometric scanning technologies; and
2. Have a written policy relating to the storage of biometric information that complies with BIPA.