

Texas employers, get ready for spike in biometric privacy lawsuits

by Jacob M. Monty
Monty & Ramirez, LLP

Since the introduction of biometric authentication technology, the number of employers using it to capture their employees' biometric data has grown. Some employers require employees to clock in and out of work using their fingerprints. Others rely on facial recognition software and retina scans to accomplish the same. While the technology offers several advantages, you should be aware of the risks that come with it.

Lawsuit against Texas-based airport services operator

Earlier this year, numerous employees filed a lawsuit in Illinois against Total Airport Services, LLC (TAS) for purportedly violating the state's Biometric Information Privacy Act (BIPA). The employees claim TAS forced them to use their fingerprints to clock in and out of work at Chicago's O'Hare International Airport without their consent.

According to the lawsuit, TAS failed to tell employees it was collecting the biometric data or obtain their consent in writing for the collection and storage. The employees further allege the employer never explained how the data would be stored and when it would be destroyed, which the BIPA requires. The lawsuit illustrates the legal risks employers take on when collecting biometric data from employees. *Kristin Nedialkova v. Total Airport Services LLC*.

Texas follows Illinois' footsteps

The Illinois BIPA, enacted in 2008, requires employers to take several steps before they can properly obtain biometric information. Under the

BIPA, they must have a policy available to the public with information on the retention schedule and guidelines for permanently destroying the biometric data they collect. They also must provide each employee with written notice that biometric information is being collected or stored. The notice must include the employer's specific purpose and length of term for the information's collection and storage. And of course, employers must obtain a "written release" from each person whose biometrics will be handled or from their legally authorized representatives.

Once biometric data is obtained, employers must use reasonable care to protect it in the same or similar way they guard other confidential information. Additionally, the BIPA prohibits employers from selling, leasing, or otherwise profiting from the biometric data they handle.

A year later, in 2009, Texas passed its Capture or Use of Biometric Identifier Act (CUBI). While the law is similar to Illinois' BIPA in many respects, there are differences. For example, the CUBI doesn't require an employee's consent to be in writing. And whereas Illinois provides individuals with a private right of action (or claim) under the BIPA, only the Texas state attorney general can file an action under the CUBI.

Nonetheless, employers in Texas must notify employees in advance that they plan to collect biometric data and obtain their consent. Employers are responsible for using reasonable care to secure the biometric data and in a manner commensurate with how they protect other similar confidential information. Similar to the BIPA, the CUBI prohibits employers from selling, leasing, or otherwise disclosing an individual's biometric identifier to another entity.

No harm, no foul? Think again

The lawsuit against TAS was filed shortly after the Illinois Supreme Court ruled against Six Flags entertainment corporation in January for improperly collecting the fingerprint data of a teenager who bought a season pass to the amusement park, without obtaining his consent. Throughout the appeal, Six Flags argued the teen had no grounds to sue because he suffered no actual damages.

The Illinois Supreme Court ruled that a violation of the law was damage enough. The court's ruling echoes the message to entities collecting biometric data: An invasion of privacy is injury enough for any employee or individual whose biometric data is being collected.

Bottom line

Texas employers seeking to collect employees' biometric information should heed the warnings offered by the recent cases that raise important privacy issues.

[Jacob M. Monty](#) is the managing partner of [Monty & Ramirez, LLP](#) and an editor of [Texas Employment Law Letter](#). He can be reached at jmonty@montyramirezlaw.com.