Collection of Biometric Data Raises Privacy Concerns for Employees and Compliance Issues for Employers

Insights
3.15.18

Many of us have become comfortable with the convenience of logging into our laptops or smartphones using a fingerprint scan in lieu of remembering yet another password. We are familiar with television and movie portrayals of retina scans being required for access to top secret laboratories or other secure buildings and rooms. This kind of technology, however, is no longer the stuff of science fiction. Businesses are increasingly using biometric data (i.e., measurements of a person's physical being) for a variety of identification purposes, such as to provide security for the financial transactions of their customers and for the tracking of work hours of their employees.

Fingerprints, retina or iris scans, voiceprints or scans of hand or face geometry are all examples of biometric identifiers. Unlike a stolen password or credit card number, biometric identifiers are unique and immutable. Thus, once compromised, the biometric identifier has forever lost its ability to be used as a secure identifying feature. In response to privacy concerns, several states have enacted legislation governing the collection, use and storage of biometric data and more states are poised to do so.

In 2008, Illinois became the first state to enact legislation concerning businesses' collection of biometric data when it passed the Illinois Biometric Information Privacy Act, 740 ILCS 14 *et seq.* ("BIPA"). Texas followed by enacting its own biometric privacy law in 2009; and in June 2017, Washington became the third state to pass a biometric privacy law. A number of other states such as Alaska, Connecticut and New Hampshire have proposed biometric data laws. At present, there is no federal law on the subject.

The Illinois BIPA imposed the following obligations on employers and other organizations:

- Organizations must provide written notice to their employees and obtain a release (i.e., authorization) from their employees prior to the collection of any biometric identifier. The notice must include the purpose of the collection and the duration that the organization will use or retain the data.
- Organizations must protect collected biometric data in the same manner they would protect other sensitive and confidential information using the reasonable standard of care in its industry.
- Organizations must have a publicly available, written policy stating how long the organization will retain the data and rules governing the destruction of that data.

BIPA prohibits organizations from selling or profiting from the biometric data they collect. It also prohibits organizations from disclosing biometric data unless: (1) they obtain consent; (2) the disclosure completes a financial transaction requested by the individual; (3) the disclosure is required by federal, state or municipal law; or (4) the disclosure is required by a valid warrant or subpoena. The BIPA provides a private right of action for violations of the statute and entitles a prevailing party to statutory damages for each violation equal to the greater of $1,000 or actual damages for negligent violations and the greater of $5,000 or actual damages for intentional or reckless violations.

The laws passed in Texas and Washington concerning biometric data are similar, but not identical to the BIPA. For example, the Texas law requires informed consent by individuals before organizations may begin collecting biometric identifiers; however, the consent need not be written. Also, unlike the BIPA, only the Texas Attorney General can enforce the Texas biometric data privacy law as the law does not provide a private right of action. Washington's biometric data privacy law applies only to biometric identifiers that are "enrolled" in a commercial database, which is defined as "captur[ing] a biometric identifier of an individual, convert[ing] it into a reference template that cannot be reconstructed into the original output image and stor[ing] it in a database that matches the biometric identifier to a specific individual." The Washington statute also expressly excludes from the definition of biometric data: "a physical or digital photograph, video or audio recording or data generated therefrom." Thus, the Washington statute likely excludes the facial recognition technology social networking and photo storage websites use to automatically tag users in digital photographs.

While BIPA appeared to fly under the radar of plaintiffs' counsel for a while, since August 2017, more than 30 class action lawsuits have been filed in Illinois alleging that the businesses failed to comply with BIPA's written notification and release requirements when they collected the biometric data of their employees, contractors, and customers. Given the landscape, employers in Illinois, Texas and Washington must take immediate steps (if they have not done so already) to come into compliance with these various biometric privacy laws. Even in states where such laws have not yet been passed, it would behoove employers to establish safe practices and be on the lookout for new developments. Using BIPA as a guide, employers should take the following steps.

1. Employers should consider providing written notice to employees and obtaining the written consent of employees before collecting, using or storing biometric data of those employees. The notice should describe the type of biometric data that is being collected, the specific purpose of the collection, and the time period during which the biometric data will be collected, used and stored.
2. Employers should consider developing and implementing a policy about the retention and disposal of biometric data.
3. Employers should protect the biometric data that they collect in at least the same manner as other sensitive and confidential information. For example, employers should use reasonable safeguards, such as encryption, in the storage or transmittal of this information.

4. Employers should establish safeguards against the sale, lease or sharing of the biometric data that they collect from their employees.
5. Employers who use third parties in the collection or storage of biometric data should include these third parties in the notice and consent provided to employees and ensure that the third parties follow appropriate standards of security.

As more states enact biometric data protections, employers are likely to see increased government enforcement and private litigation and would be well advised to keep abreast of new compliance obligations.