THE
NATIONAL LAW REVIEW

Be Prepared for the Next Wave of Biometric Data Laws: Five Tips for Businesses

Wednesday, March 20, 2019

Article By Carlton FieldsInsights
Joseph W. Swanson

Civil Rights
Consumer Protection
Litigation / Trial Practice
Illinois

Advancements in technology have made it possible for more companies to use biometric data to streamline their business, improve security and workplace efficiency, and offer new services and features to customers. Biometric data broadly consists of any information that can be used to identify a person based on biometric identifiers, such as fingerprints, retina scans, and facial geometry. Real-world applications for this type of technology are endless, from smartphones activated by facial recognition, to employee time-management processes that rely on fingerprints in lieu of traditional punch-clock cards.

Although biometric technology offers myriad opportunities to streamline business processes and offer new services, that technology also carries with it increasing regulatory and litigation risk. Congress and state legislatures are considering new laws to regulate the collection and use of personal data, including biometric data. Currently, there is no federal law that regulates the collection and use of biometric data, but its use could implicate existing federal laws, including HIPAA and the Fair Credit Reporting Act, among others. Additionally, it is unknown whether and to what extent the various federal data privacy laws under consideration at the national level would regulate the use of biometric data or preempt state laws. Three states have enacted biometric data privacy laws: Illinois, Texas, and Washington. But the Illinois Biometric Information Privacy Act (BIPA) is the only one to provide for a private right of action, whereas the Texas and Washington statutes are enforced by the state attorneys general.

We recently issued a client alert on Illinois' BIPA following the much-anticipated ruling in *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 (Jan. 25, 2019). In *Rosenbach*, the Illinois Supreme Court held that a plaintiff suing under BIPA need not allege or show actual injury or an adverse effect to maintain an action for damages under the statute. This is important because BIPA allows for $1,000 or $5,000 in statutory damages per violation, depending on whether the violation was negligent, intentional, or reckless. As anticipated, the *Rosenbach* decision has already resulted in a sharp increase in class action lawsuits, many of which have been filed against employers for their use of biometric data in the workplace. Some companies have even altered their behavior as a result of this law. For example, Nest, the maker of smart thermostats and doorbells, reportedly deactivated a feature of their popular doorbells in Illinois, lest that feature draw the ire of plaintiffs' attorneys.

States without biometric information regimes may still regulate under common law or privacy-related statutes, but a handful of other jurisdictions have proposed, or are currently considering, biometric data privacy legislation with varying requirements, including Alaska, Arizona, Connecticut, Delaware, Florida, Massachusetts, Montana, New Hampshire, and New York City. Some of these proposed statutes would include a private right of action like Illinios' BIPA, while others would be enforced by the state's attorney general. The new law introduced in Florida, HB 1153 and SB 1270, is patterned after Illinois' BIPA and, as first introduced, it would allow for a private right of action. It would not permit businesses to "collect, capture, purchase, receive through trade, or otherwise obtain" biometric data without written notice and consent from the individual.

Given the extraterritorial reach of Illinois' BIPA and the fact that other jurisdictions are likely to enact their own versions of it, companies would be wise to evaluate their practices and policies related to the collection and use of biometric data. Specifically, businesses should undertake the following:

1. Evaluate the extent to which the organization and its vendors collect and use biometric data from its employees and consumers. Review vendor agreements for indemnification and employee training provisions, if applicable.
2. Obtain written and informed consent from the employee or consumer prior to the collection and use of biometric data, setting forth the specific purpose and length for which the data will be used and held.
3. Develop a written policy to govern the collection and use of biometric data that sets forth the purposes and scope of the collection and use of the data, as well as the means for retaining and deleting the data after its life cycle.
4. Remember to update any outward-facing privacy policies to reflect any personal information being collected or processed as a result of new product lines or ventures, including biometric data.
5. Consider whether it is necessary to update the company's data incident response plan to include biometric data as information that, if exposed, would trigger notice requirements.

Source URL: https://www.natlawreview.com/article/be-prepared-next-wave-biometric-data-laws-five-tips-businesses