

What To Do Next With Biometric Information in Illinois?

February 22, 2019

With the Illinois Supreme Court's recent decision in *Rosenbach v. Six Flags Entertainment Corp.*, the floodgates have opened for class actions in Illinois against businesses that collect biometric information from employees or customers. In *Rosenbach*, the Illinois Supreme Court decided that alleged procedural violations of Illinois's Biometric Information Privacy Act ("BIPA") are enough, without alleging actual injury to an individual, to bring an action under the law. While the particular details of that decision can be relevant to specific situations, if your company currently is collecting biometric information from customers or employees, or considering doing so in the near future, you need to know what to do now in light of this new ruling.

If your company has been collecting biometric data:

- Conduct a rapid internal audit to determine how your company, or any agent or contractor you hire, is using biometric data for any reason (e.g., security for facilities or devices, time clock or other employment verification, or marketing to consumers).
- Once you understand the scope of biometric data collection, implement BIPAs requirements, which include: (1) informing an individual that his or her biometric information is being collected or stored; (2) informing the individual of the purpose for the collection, storage, or use and how long such information will be collected, stored, or used; and (3) receiving a written release from the individual to collect the information.

Since the *Rosenbach* ruling, we have seen a rapid increase in the number of BIPA class action lawsuits filed. If your company is currently facing a lawsuit over an alleged BIPA violation, consider taking the following steps:

- Remove the case to federal court. Based on Supreme Court precedent and a recent decision from an Illinois federal court, defendants facing these class actions may be able to challenge a plaintiff's standing to bring suit based solely on a procedural violation of the statute where no actual harm has occurred.
- Identify sources of either express or implied consent for the collection of biometric information. For example, employees may have received notice from an employee handbook about collection of their biometric data.
- Assert class action defenses related to typicality and commonality. Typicality is meant to ensure that the named plaintiff's claims have the same essential characteristics as the claims of the entire class. If proof of the named plaintiff's claims would not necessarily prove all of the proposed class members' claims, plaintiff fails the typicality requirement. Commonality requires plaintiffs to demonstrate that the class members have suffered the same injury, meaning that

they were affected by the same violation of the same statute. This emphasis on dissimilarities between plaintiffs will illustrate whether there are any class-wide commonalities.

Finally, companies considering biometric data collection in Illinois should:

- Prepare explicit disclosures and documents for written consent to collect as required by the BIPA.
- Determine whether collection of biometric data is truly necessary for the business, given the strict requirements of the BIPA and increase in the number of lawsuits. If this data is necessary, collect as little as possible and consider and whether it can be captured and not retained.
- Avoid collection of biometric data in Illinois. Some companies have begun altering their behavior in Illinois to adhere to the law. For example, Nest, a maker of smart thermostats and doorbells, sells a doorbell with a camera that can recognize visitors by their faces. However, Nest does not offer that feature in Illinois because of the BIPA.
- Keep an eye on legislative developments. Many other states have considered biometric privacy legislation over the years, but only Texas (in 2009) and Washington (in 2017) have passed such laws. But that may change soon. In the first few weeks of 2019 alone, legislators have already introduced new bills in Arizona, Connecticut, New Hampshire, New Mexico, New York, Oregon, and Washington. These initiatives have the potential to introduce a conflicting national patchwork of regulations.
- In Illinois, there is currently a bill (SB3053) pending before the Illinois legislature to amend the BIPA. The bill proposes to exempt private entities from the BIPA's requirements under a number of circumstances, including (1) if the biometric information is used "exclusively for employment, human resources, fraud prevention, or security purposes," (2) if the company "does not sell, lease, trade or similarly profit" from the biometric information, or (3) if the company protects biometric information at least as securely as it secures other sensitive information.

If you have additional questions or need assistance, please contact:

[Randall Lehner](mailto:rlehner@kelleydrye.com) (312) 857-7238 rlehner@kelleydrye.com

[Janine Fletcher-Thomas](mailto:jfletcher@kelleydrye.com) (312) 857-2507 jfletcher@kelleydrye.com