Illinois Supreme Court to Decide Biometric Privacy Case

Labor & Employment Law Update

on November 27, 2018

In October of 2017, we first reported on the filing of a class action suit by a group of Chicago-area employees where plaintiffs alleged that their employer's use of worker fingerprints for time-tracking purposes violates the Illinois Biometric Information Privacy Act (BIPA). Specifically, the employees claimed that their employer failed to properly inform them in writing of the specific purpose for which their fingerprints were being collected and the length of time their fingerprints would be stored. Plaintiffs also claimed the employer failed to obtain written consent before obtaining fingerprints.

Then, this past June, we reported on a federal court's decision finding that despite no concrete damage, an employee (and her putative class) might have a triable cause of action for violating her privacy and right to control her biometric data. The allegations in this case also included a failure to inform the specific purpose of collection and failing to obtain written authorization for the collection of biometric data.

On November 20, 2018, the Illinois Supreme Court heard oral arguments in a *Rosenbach v. Six Flags Entertainment Corp.*, a case specifically addressing BIPA. While *Rosenbach* is not an employment case (it concerns a patron's access to Six Flags), it nevertheless involves the issue of whether collection of biometric data alone triggers statutory damages even if the plaintiff has not claimed actual harm. The lower appellate court in *Rosenbach* found that alleging only technical violations of the notice and consent provisions of the statute is not tantamount to alleging an adverse effect or harm. Thus, how the Illinois Supreme Court rules in the next few months is bound to have a significant impact on Illinois employers and potentially elsewhere in the country.

In the meantime, to avoid and/or minimize any BIPA issues or potential liability, we continue to recommend that employers take the following steps:

1. Establish a written policy that addresses the purpose(s) of biometric data use, how it will be collected, and how it will be stored.
2. Be prepared to address any requests for reasonable accommodations based on disability, religious, or other reasons.

3. If biometric data might leave a closed system, ensure that proper safeguards are in place, including contractual liability shifting.
4. Ensure that employees whose biometric data is used acknowledge the policy, and authorize its use and collection.
5. Train supervisors on the company's policies and practices to ensure consistency.
6. Have biometric data systems audited to ensure that data is not open to the public or a systems breach.
7. Finally, consult with competent employment counsel to ensure that policies and practices comply with relevant law.