More Technology, More Headaches for Employers

Labor & Employment Law Update

on June 7, 2018

Technology is great. I can use my smartphone to change a million TV channels without getting up (of course, there's still nothing to watch until Game of Thrones returns).

Employers, too, are reaping the benefits of technology for the most routine areas of employee and facilities management – including timekeeping and building security. But with the transitions from handwritten and manually punched time cards to fingerprint scanner timeclocks, and mechanical keys to retinal scanners, employers face significant risk under privacy laws.

As a result, many states are beginning to pass employee privacy laws related to biometric data (including but not limited to retina or iris scans, fingerprints and voiceprints, and hand and face geometry). And with laws and regulations, comes the need for compliance to stave off lawsuits, including private causes of action and class actions.

For example, a Federal Court in Illinois recently found 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 employer and its timekeeping vendor allegedly failed to:

- inform the employee of the specific purpose or length of time fingerprints were to be collected, stored or used;
- make available any biometric data retention policy or guidelines (if there was one);
- obtain employee releases and authorizations for the collection and use such biometric data;
- and implement reasonable procedural safeguards.

The employer is further alleged to have systemically disclosed the biometric data by sharing it with the timekeeping vendor.

Biometric Data Done Right

Biometric data is not something to be afraid of, as long as it is administered and used appropriately. The following key steps can help businesses ensure that they are complying with relevant laws:

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 there are proper safeguards 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 the 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.

More Technology, More Headaches for Employers