Legal Pitfalls for Employers Using Biometric Technology in the Workplace

ATTORNEYS

Nathan A. Lennon
859.426.7222
nlennon@reminger.com

PRACTICE AREAS

Employment Practices Defense

Employment Newsletter, November 2019
Nov 2019

As often happens, the state of the law lags behind social and technological developments, resulting in potential conflicts and pitfalls for the unwary. One new potential area of conflict that all HR professionals should be aware of is the legal implication of the use or dissemination of employee biometric data. With advances in technology, increasingly employers are using biometric data in numerous areas of business in an effort to increase employee productivity. For instance, biometrics, in the form of fingerprint and facial recognition, are often used as security measures to restrict access to facilities or data systems. In addition, as many HR professionals are aware, the increasing trend for several years now has been to encourage employees to undergo annual voluntary biometric screenings as a part of employer-sponsored health insurance programs. The use of biometrics and biometric data has even begun to penetrate the consumer electronics market - as everyone knows by now, even cell phones use biometric data to lock and unlock access to the phones.

Given greater access to unique data about employees – whether in the form of facial recognition, fingerprint data, or voice recognition, employers might be tempted to use this data in ways that could lead to potential legal exposure. For example, one such potential scenario could arise where an employer is tempted to share biometric data collected during employment or in an internal company investigation with law enforcement in an effort to protect its interests from internal theft of intellectual property. If the employer can tie access to company property to the unique identifier of an employee's fingerprints or facial geometry, this type of evidence would be particularly helpful for law enforcement in a criminal investigation.

Unfortunately, even in a scenario like this, where the employer might feel justified in sharing this unique identifying information with law enforcement, HR professionals should tread very carefully. Numerous states, including Washington, Texas, and Illinois, have biometric data privacy acts. Although the protections vary by state, of course, many of these acts require consent of the employee to collect biometric data, and notification when that data is shared with third parties. Although Ohio and Kentucky do not have biometric privacy laws as such, Kentucky has recently adopted a notification statute that requires

essentially any business in Kentucky experiencing a data breach of customer or employee information (including specifically biometric data) to inform the third-party of the breach. *See* KRS 365.732.

In addition to state laws which are specifically beginning to protect biometric data, existing federal law likely would come into play as well. The Health Insurance Portability and Accountability Act ("HIPAA") was initially enacted to protect private health information of patients, and is recognized as an important privacy concern in the employment context as well. Protected health information under HIPAA is generally regarded to include individual patient identifiers, including fingerprints and retinal scans. Beyond these "outer" identifiers, with the rise of the use of genetic testing, congress extended many of the protections of HIPAA to pure "genetic" information, through the Genetic Information Nondiscrimination Act "GINA". Although nominally concerned with prevention of employment discrimination based on genetic information, the GINA's statutory reach extends to literally any manifestation of disease in an individual or the family member of an individual, regardless of whether such disease has a genetic basis or not.

Given the thicket of state and federal laws governing the use and dissemination of biometric data, any employer should be very careful in voluntarily sharing employee biometric data with law enforcement, or frankly anyone else. As previously noted, in Illinois and several other states this data essentially cannot be shared at all without employee consent. And even in Kentucky, an employer would likely have to notify the employee about any data breach of employees' biometrics. Finally, due to the personally-identifiable nature of any employee's biometric data, it appears that HIPAA would prevent this dissemination absent a court order, subpoena, or employee consent.

In conclusion, with the maze of local and national laws applicable to employee biometric data, if an HR professional believes that it might be necessary to share the biometric data of an employee with law enforcement or anyone else, the first call that professional should make is to an attorney, to assist in guiding them through this legal minefield. The employment attorneys of Reminger are available all throughout Ohio, Kentucky, and Indiana to assist in this area or with any other labor and employment needs that you may have.