Assessing the Fine (Finger) Print:
Biometric Data is the New Frontier In Data Security and the Next Wave of Litigation

BY EMILY KNIGHT

Using an employee's biometric data — such as fingerprints and facial recognition — as a means of security is quickly gaining popularity among employers. However, as more states begin to regulate the collection and handling of this ultra-personal data, employers may find themselves exposed to liability. Given the evolving and uncertain regulatory landscape surrounding biometric data, this article will explore how Ohio employers can utilize cutting-edge security measures while still protecting themselves from future litigation.

What Is Biometric Data and Why Collect It

Biometric identifiers are the distinctive, measurable characteristics used to recognize or describe an individual. This includes fingerprints, voiceprints, and iris or retina scans. Biometric data is the information derived from the identifiers, usually reduced to algorithms or mathematical equations. Biometric identifiers are what the employer actually collects — e.g. the fingerprint. But biometric data is the information the employer digitally stores and uses. Employers favor biometric data for security purposes because of its increased reliability and efficiency. Employers are also increasingly incorporating biometrics into their day-to-day operations to protect against potential FLSA wage and hour claims. By using a "biometric" timeclock, for instance, employers can significantly reduce the amount of buddy punching and other manipulative practices. But unlike knowledge-based, personal information (credit card numbers, passwords, etc.), biometric data cannot be replaced if compromised. The privacy implications are significant, but the law in this area is largely unchartered. As a result, employers wanting to explore this new frontier should do so carefully.

The Current Regulatory Landscape

Illinois, Texas, and Washington are the only states that have enacted statutes regulating biometric data. Currently, no federal law regulating biometric data exists. Illinois' Biometric Information Privacy Act (BIPA) offers the most protection, but all three statutes create a complex regulatory scheme that imposes additional burdens on the employer.

Scope of the Statutes

The BIPA and Texas statutes cover any information based on an individual's biometric identifier and is used to identify an individual, including hand and face geometry. But Washington's statute expressly excludes hand and face geometry. This is likely in response to recent class-action suits alleging social media companies violated BIPA by using facial recognition programs without the users' permission. Also, the Texas and Washington statues apply to data collected for commercial purposes, and in Texas, this includes security purposes. The BIPA does not have this limitation and applies to any purpose an employer might have for collecting the data.

Collecting, Storing, Sharing, and Destroying Data

Before collecting biometric identifiers, employers must provide notice and obtain consent. In Illinois, notice and consent must be written, explain the purpose for collection, and identify the retention period. Typically, employers must destroy the data once the purpose has expired or three years after the employee leaves the company. In Washington, notice and consent do not have to be written but must be "readily available" to employees, and employers may only store the data as long as reasonably necessary. Texas only requires notice be given and consent obtained, and employers must destroy the data within a "reasonable time" but not later than one year after it is no longer needed. All three statutes require the employer to protect the data in at least the same manner it protects other sensitive and confidential information. And all three statutes generally prohibit selling and/or profiting from the data, although some enumerated exceptions exist.

Penalties

The state attorney general enforces the Texas and Washington's statutes. But the BIPA is much more generous to employees. The BIPA creates a private right of action entitling a plaintiff to statutory damages and attorney's fees. For negligent violations, plaintiffs may receive the greater of $1,000 or actual damages for each violation. For intentional or reckless violations, plaintiffs may receive the greater of $5,000 or actual damages for each violation.

Ohio

Ohio has enacted a data breach notification statute. But this statute only applies to personal information and does not capture biometric data — at least in its current form. Although Ohio is not the only state that has yet to address this issue, some states are beginning to assess regulations. In fact, Alaska, Connecticut, and New Hampshire all have proposed legislation similar to the BIPA. There is no indication as to whether Ohio will propose biometric data legislation in the near future, but as more states enact legislation it behooves employers to begin thinking about compliance now.

Federal and International Laws

Even without a regulatory scheme, Ohio employers may still face liability for improperly collecting or using biometric data under federal law. Section 5 of the FTC Act grants the FTC broad authority to protect consumers from unfair and deceptive trade practices in or affecting commerce. Under Section 5, the FTC may take enforcement action against commercial organizations that engage in unfair or deceptive trade practices involving biometric information. For example, if a company promises a certain level of security but fails to keep this promise, the FTC may take action

regardless of whether the company violated an Ohio statute. Employers should also keep in mind EU's General Data Protection Regulation (GDPR) that takes effect May 25, 2018. The GDPR broadly prohibits processing biometric data of any EU citizen unless it fits into one of the explicitly enumerated bases such as consent, the performance of specific contracts, or processing for certain specific circumstances.

The First Wave of Litigation

In recent years, Illinois companies have begun to experience an influx of class-action litigation under the BIPA. In this litigation, two types of fact patterns have emerged: (1) improper use of facial recognition technology (e.g. social media); and (2) improper collection and use of fingerprints, primarily in the employment context. Specifically, plaintiffs are alleging that their employer failed to provide proper notice and/or obtain consent before collecting their fingerprints. The potential liability for employers in these types of cases can be significant.

In 2016, L.A. Tan settled with a class of plaintiffs for $1.5 million, agreeing to pay $600,000 in attorneys' fees. And in 2017, a class of plaintiffs sued Roundy's Supermarket — operator of Mariano's and subsidiary of Kroger's — for $10 million in damages. Employers have challenged some of these class actions, particularly on the issue of standing. Yet, the courts' willingness to accept this challenge has been mixed.

Article III Standing

Plaintiffs seeking redress against employers are not alleging any theft or misuse of their biometric data. Instead, these suits rely on allegations of improper collection — a technical violation. In several instances, courts have dismissed cases relying on technical violations on the grounds that cognizable injury-in-fact does not exist. *See McCollough v. Smarte Carte, Inc.,* 2016 WL 4077108 (Aug. 1, 2016). But in *Monroy v. Shutterfly*, Inc., 2017 WL 4099846 (Sept. 15, 2017), the court determined that the mere invasion of privacy associated with the defendant's collection of biometric information without the plaintiffs' knowledge or consent was a sufficient injury-in-fact to give rise to standing. In *McCollough,* the plaintiffs voluntarily provided their employer with the data. But in *Monroy*, the employer obtained the data unbeknownst to the employees. The court in *Monroy*, relied on this distinction in reaching its conclusion. The BIPA also requires a cognizable harm, loss, or injury, but this area of law remains unchartered.

What Ohio Employers Can Do Now to Avoid Liability Later

The absence of biometric data statutory schemes is not an excuse for employers to ignore their biometric data practices. As more employers incorporate this data into their day-to-day operations, it is almost certain more states will begin to regulate. Therefore, employers seeking to avoid future liability but also integrate this new technology should begin updating their data security policies and procedures now. Although the regulatory landscape remains unclear, there are a few things employers can implement now to avoid headaches later.

Employers thinking about using biometric data (or already using it) should consider what the biometric data is used for. Using it for non-commercial, security purposes is likely to pose less of a risk compared to using it in consumer transactions. Also, employers should only collect biometric identifiers after providing written notice and obtaining informed consent. This notice and consent should detail the purpose of collecting, how the data will be used, the company's retention policy, and whether any outside vendors will have access to it. Since almost all biometric data litigation in the employment context right now hinges on notice and consent, it is vital employers sufficiently address this step.

Employers must also protect this highly sensitive data *at least* in the same manner as other sensitive and confidential information. This means encryption, limited access, and retention and disposal policies. Lastly, employers should consider adopting safeguards for the sale, lease, or sharing of this data. And if this data is shared, disclose it to the employee prior to collection. Remember, creating these policies is not enough. Employers must actively carry out these procedures or face action by the FTC.

Despite the recent uptick in class-action litigation, biometric data is not going anywhere. Instead, it is likely that more and more employers will incorporate this cutting-edge technology into the workplace. As of now, this area of law remains largely untouched. But a prudent employer will begin addressing its biometric data privacy policies and procedures now to avoid potential exposure to class action litigation later.

Emily Knight is a member of the Tucker Ellis Trial Department. She has been a CMBA member since 2017. She can be reached at (216) 696-4893 or emily.knight@tuckerellis.com.