Littler
Employment & Labor Law Solutions Worldwide®

Dear Littler

DECEMBER 6, 2017

DEAR LITTLER: WHAT DOES OUR COMPANY NEED TO DO BEFORE WE BEGIN USING BIOMETRIC TIMECLOCKS?

By: Philip L. Gordon and Kwabena A. Appenteng

Dear Littler: We are going to replace the punch-card timeclocks in our U.S. facilities with timeclocks that allow employees to "clock in" each day using their fingerprint. I've read about a flood of recently filed class action litigation against companies that collected biometric information and understand that many of these cases have been filed against employers that use biometric timeclocks. Can we go ahead and roll out the timeclocks? Or is there something more that we need to do?

— *Concerned in Chicago*

Dear Concerned in Chicago,

Your question is a good one, and of topical interest. The recent rash of class actions against employers that use timeclocks that collect information about employees' fingerprints highlights the importance of understating the relevant laws, and planning ahead before replacing your company's current system.

The timeclock that your company intends to use is a "biometric timeclock." This timekeeping technology uses a scan of an employee's body feature, such as a fingerprint, retina or iris, to verify the employee's identity and clock the employee into, and out of, work. Biometric timeclocks prevent timeclock fraud, increase timekeeping efficiency, and enhance the accuracy of wage calculations.

However, as illustrated by the mounting number of class action lawsuits, implementing a biometric timeclock system must be done with care. There are several laws that govern the collection and storage of biometric information. These laws may require your company to, among other things, obtain written consent from employees before collecting biometric information from them. Here is a summary of key considerations.

Understand the Data Collected by the Biometric Timeclock

Your company's legal obligations will depend on the type of information the biometric timeclock collects and the states in which your company rolls out the timeclock. Not all states regulate biometric timeclocks, and the state laws differ based on the type of information that the timeclock collects. Let's focus on the timeclock first.

You will find many different types of biometric timeclocks on the market, and they use differing technology. Timeclocks that require employees to place a finger on the device are most common, but face-scanning and iris-scanning technology is also available. Another key difference is whether the technology collects an image of the body feature itself, such as a photograph of an actual fingerprint, or creates a unique identifier based on the body feature. For example, many models do not store an exact image of an employee's fingerprint. Instead, the timeclock measures the distance between points on the fingerprint and then applies an algorithm to create a mathematical representation of the employee's fingerprint. This "template" is linked to the employee's identity. Each time the employee clocks in or out, the biometric timeclock applies the same process to the fingerprint and compares the result to the template to confirm the identity of the person who clocked in or out.

State Laws Regulating the Collection of Biometric Information

Over the past year, biometric privacy legislation has been introduced in several states, including most recently in Michigan.[1] To date, however, only three states have enacted biometric privacy laws: Illinois, Texas, and Washington State. Washington's law, effective July 23, 2017, is the most recent, but the law does not apply to an employer's use of a biometric timeclock as part of a timekeeping system. Washington's law applies when biometric data is stored in a database for a "commercial purpose," which is defined as "a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services." Therefore, only the biometric privacy laws in Illinois and Texas are relevant for your company's purposes. In addition to these biometric privacy laws, New York's Labor Code includes a provision governing fingerprinting of employees that is applicable to biometric timeclocks. Here's a summary of each state's law:

Illinois

Illinois' Biometric Information Privacy Act (BIPA)[2] was enacted in 2008 and is the broadest, and most prescriptive, of the three biometric privacy laws. As a result, we are currently seeing BIPA class actions being filed against employers in Illinois courts on a weekly basis.

BIPA requires that private entities obtain employees' consent before scanning their "biometric identifiers" or collecting "biometric information" using a biometric timeclock. What makes BIPA so restrictive is its expansive application. BIPA defines a "biometric identifier" as a scan of an individual's fingerprint, retina or iris, or a scan of an individual's hand or face geometry. BIPA also applies to "biometric information," which is defined as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." This means even biometric timeclocks that do not store an image of the biometric identifier, but instead create a template or unique identifier based on the image, fall within the scope of BIPA.

1 *See* Michigan House Bill No. 5019.
2 740 ILCS 14/1 *et seq.*

Two recent Illinois federal court opinions illustrate BIPA's broad scope. Those opinions held that BIPA can apply to technology that scans ***photographs of faces*** because the resulting measures of facial geometry constitute "biometric identifiers" as defined by BIPA.[3] Against this backdrop, it is unlikely that your company will be able to avoid BIPA's application to its biometric timeclock, regardless of the technology it utilizes.

Under BIPA, before your company can collect, capture, or obtain an employee's biometric identifier or biometric information (jointly, "biometric data"), it must *first* provide employees with a written notice that informs them of the following:

- That their biometric data is being collected and stored;
- The company's purpose for collecting, storing, and using employees' biometric data;
- The length of time that employees' biometric data will be retained.
- The employer must obtain the employee's written consent to the collection and use of their biometric data as described in the notice.

In addition to this notification requirement, BIPA requires employers to:

- Make available to all employees a written policy that (1) establishes a retention schedule for the biometric data and provides for secure destruction of the biometric data at the earlier of the termination of the employment relationship or within three years of the employee's last interaction with the company; and (2) explains how employees' biometric data will be destroyed.
- Establish safeguards for the biometric data that are at least as stringent as those established for the organization's other confidential information.[4]

While complying with these requirements may seem burdensome, the cost of non-compliance could be steep. BIPA provides that a successful employee may recover liquidated damages of up to $5,000 for each *violation*.

However, it remains unsettled whether employees must at least show a material risk of harm in order to maintain a claim under BIPA. There is a split on this issue in federal court. The federal appellate court in New York and a federal district court in Illinois have held that an employee cannot maintain a BIPA claim by merely alleging a failure to comply with the law's notice and consent requirements. Instead, employees must allege a material risk of harm.[5] However, an Illinois federal judge recently held that an individual who, in addition to not being given notice and providing consent, "credibly allege[d] an invasion of his privacy" through the collection of his biometric information, had alleged enough harm to maintain a BIPA class action.[6]

---

3 *See Rivera v. Google Inc.*, 238 F. Supp.3d 1088, 1100 (N.D. Ill. 2017); *Monroy v. Shutterfly, Inc.*, No. 16C10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017).

4 Failure to comply with this requirement could trigger obligations under a state's data breach notification law if biometric data is compromised. Several states, including Illinois, Iowa, Delaware (effective 4/4/18), Maryland (effective 1/1/18), Nebraska, New Mexico, North Carolina, Oregon, Wisconsin, and Wyoming, require entities that suffer a security breach involving unencrypted biometric information to comply with the state's data breach notification law.

5 *See McCollough v. Smarte Carte, Inc.* No. 16 C 0377, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016); *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499 (S.D.N.Y. 2017); *Vigil v. Take-Two Interactive Software, Inc.*, No. 17-303, 2017 U.S. App. LEXIS 23446 (2d Cir. Nov. 21, 2017) (affirming district court's dismissal of BIPA claim for lack of standing). For more information about the Second Circuit's decision and standing in BIPA cases, please refer to the following Littler article: Kwabena A. Appenteng and Philip L. Gordon, *The Second Circuit Provides A Roadmap For Employers Defending Claims Under Illinois' Biometric Information Privacy Act*, Littler Insight (Dec. 6, 2017).

6 *See Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *8, n. 5 (N.D. Ill. Sept. 15, 2017).

Notably, in February of this year, the Illinois General Assembly introduced a bill to amend BIPA to permit employers to collect biometric information "to the extent necessary for an employer to conduct background checks or implement employee security protocols."[7] The bill was referred to the Rules Committee in March and is currently pending. It is unclear at this point whether an employer's timekeeping system will qualify as an "employee security protocol," but if so, the passage of this bill may reduce the burden BIPA currently places on employers.

Texas

Texas' biometric privacy law[8] applies only to "biometric identifiers," which are defined to include fingerprints, retina or iris scans, voiceprints, or a "record of hand or face geometry." Therefore, in Texas, your company can avoid application of the biometric privacy law by using biometric timeclock technology that collects only information based on an analysis of the biometric identifier, such as the distance between points on a fingerprint.

Whereas BIPA applies to the collection, capture, or obtaining of biometric data for any purpose, Texas' law is restricted to biometric identifiers that are "captured" for a "commercial purpose." However, this term is not defined in Texas' law, or any attendant regulations.

Like BIPA, Texas' law requires that employees are notified about the collection of their biometric information and that employees give consent to the collection. Unlike BIPA, Texas' law does not require your company to disseminate a retention schedule or policy document. Also, Texas' law does not provide employees with the right to file a lawsuit based on a violation of the law, but it does permit Texas' attorney general to bring suit, and seek up to $25,000 in damages for each violation.

New York

Section 201-a of New York's Labor Law prohibits employers from requiring the fingerprinting of employees "as a condition of securing employment or of continuing employment."[9] In April 2010, the New York Department of Labor (NYDOL) issued a response to a "Request for Opinion" on whether the use of a biometric timeclock device violates this New York law. The NYDOL explained what the statute prohibits: (1) requiring employees to use a biometric timeclock that requires a fingerprint to clock in will likely violate Section 201-a, *even if the device does not store the actual fingerprint*; (2) taking adverse action against an employee who refuses to use a fingerprint to clock in; and (3) "coercing" employees to use a biometric timeclock that requires a fingerprint to clock in is not permitted. However, the NYDOL made clear that the statute *permits*: (1) voluntary fingerprinting of employees; and (2) instruments that measure the geometry of a hand that do not scan the surface details of the hand and fingers.

Implementing a Biometric Timeclock System in the European Union

While your company is currently focused on rolling out biometric timeclocks in its U.S. locations, if the company intends to eventually do the same at its EU subsidiaries, you should be aware of impending changes to the EU's data protection framework that may frustrate this plan.

7 Illinois HB 2411 (2017).
8 Tex. Bus. & Com. Code Ann. § 503.001.
9 NY Labor § 201-a.

On May 25, 2018, the current data protection framework, known as the European Union Data Protection Directive (the "Directive"), will be replaced by the General Data Protection Regulation (the "GDPR"). Under the GDPR, biometric information will be considered a "special category of personal data," which cannot be processed unless an employer has a recognized, lawful basis for the processing. In the context of biometric timeclocks, the only justification that likely would apply is if the employee has "given explicit consent to the processing … for one or more specified purposes." However, this consent must be "freely given," and the European advisory body on data protection and privacy (the "Article 29 Working Party") takes the position that in the employment relationship, consent generally cannot be freely given because of the potential "prejudice that arises from the employee not consenting."[10] For this reason, we recommend that you consult with counsel before rolling out biometric timeclocks in the EU.[11]

In sum, your company can implement biometric timeclocks in most states without restriction. However, if your company has facilities in Illinois, New York, or Texas, your company will need to take steps to avoid violating state law.

10 *See* WP29, *Opinion 2/2017 on data processing at work*, WP 249, adopted 8 June 2017.

11 For more information about the GDPR's application to employers, please refer to the following Littler article: Philip L. Gordon, *The Next HR Data Protection Challenge: What U.S. Multinational Employers Must Do To Prepare for the European Union's Impending General Data Protection Regulation*, Littler Insight (Sept. 13, 2017).