November 15, 2018

Press Pause Before Using Biometric Tech In The Workplace

By Robert Quackenboss and Madalyn Doucet

Published in Law360


In *Byczek et al. v. Xanitos Inc*., a new class action filed recently against a hospital housekeeping company, employees allege their employer's fingerprint scanning time-tracking system runs afoul of privacy laws. The Pennsylvania-based company Xanitos Inc. now faces the lawsuit in federal court in Illinois, claiming the company violated the state's Biometric Information Privacy Act, or BIPA. The lawsuit serves as a reminder and a cautionary tale to employers considering the use of biometric data in the workplace.

The Case Against Xanitos

Xanitos employees claim that the company failed to obtain their written consent, failed to inform them of the purpose and length of time for which their fingerprints were being collected, and failed to provide a retention schedule and guidelines for destroying their fingerprint data, all in violation of the BIPA.

"While there are tremendous benefits to using biometric time clocks in the workplace, there are also serious risks. Unlike key fobs or identification cards … fingerprints are unique, permanent biometric identifiers associated with the employee," the potential misuse of which "exposes employees to serious and irreversible privacy risks," according to the complaint.

The class seeks liquidated damages of $1,000 per violation, injunctive relief and attorneys' fees and expenses.

The Illinois Biometric Information Privacy Act

Illinois has one of the strongest biometric privacy laws in the country.[1] The BIPA governs both "biometric identifiers" — defined as eye scans, fingerprints, voiceprints, or hand or face scans — and "biometric information," which is any information, regardless of how it is captured, based on an identifier and used to identify an individual.[2] The law requires employers to take three major steps before using employee biometric information, such as fingerprints:

1. ***Establish a Written Policy:*** A private entity in possession of biometric data must develop a written policy. The policy must establish a retention schedule and guidelines for destroying

biometric information when the initial purpose for collecting it has been satisfied, or within three years of the individual's last interaction with the private entity. The policy must be made available to the public.

2. ***Provide Proper Notice:*** Before a private entity may collect, capture or otherwise obtain a person's biometric data, it must inform the subject in writing (1) that biometric information is being collected or stored, and (2) of the specific purpose and length of term for which biometric information is being collected, stored and used.

3. ***Obtain Written Consent:*** Finally, before collecting or obtaining biometric data, a private entity must receive a written release executed by the subject.

BIPA also contains prohibitions on the disclosure or dissemination of biometric data without consent and requires certain protections for the storage and transmittal of the data to prevent disclosure. The law provides a private right of action, which allows for recovery of $1,000 liquidated damages, or actual damages, for each negligent violation, and $5,000 or actual damages for each intentional or reckless violation, as well as attorneys' fees and costs and injunctive relief.[3]

Other Developments in Biometric Privacy Legislation

A similar law exists in Texas, which governs employer use of biometric data.[4] Unlike Illinois, Texas law only governs "biometric identifiers," which are defined similarly to BIPA. The Texas law contains similar notice and consent requirements, but does not require a written policy governing the employer's use of biometric data. And, Texas provides no private right of action under the statute, instead permitting Texas's attorney general to bring suit seeking up to $25,000 in damages for each violation.

Washington is the most recent state to pass a biometric privacy law,[5] but the law does not apply to employers' use of employees' biometric data. Instead, it applies when biometric data is stored in a database for a "commercial purpose," meaning in furtherance of sale or disclosure to third parties. In the case of a fingerprint-based time clock, employers would not be collecting employee data for the purposes of selling or disclosing it to a third party.

Many other laws governing employers' use of biometric data have been proposed in several other states, including Alaska,[6] Michigan,[7] Montana[8] and New Hampshire.[9] Still other states have sought to explicitly add biometric data to their existing security breach laws.[10]

Lessons for Employers

The ever-changing legal landscape of collecting or using biometric data, and the potential liability it can cause, should give employers pause when considering biometric timekeeping systems, or other uses of biometric data in the workplace. There are dozens of fingerprint time clock software companies and systems advertising many benefits to employers: saving time, promoting efficiency, increasing accuracy and eliminating "buddy punching" — the practice of one employee having another punch them in or out — for example. Employers should be mindful of several legal considerations that come with using employees' biometric data:

- State laws, like those in Illinois, Texas and Washington, that impose specific protections for biometric data;

- Data breach notification laws, which could require an employer to notify an employee if his or her biometric information is exposed through a data breach;

- Laws prohibiting employers from requiring their employees to submit to fingerprinting generally, such as in New York; and

- General liability for negligence or invasion of privacy, especially if an employer fails to protect and secure biometric data.

For employers that already have or are interested in implementing a fingerprint-based time clock system, or any other procedure in the workplace that requires the collection or use of employees' biometric data, consider the following best practices:

- Maintain a written policy governing your use of biometric data. The policy should explain your purpose for obtaining biometric information, how the company will use that information, retention policies and destruction procedures, and information about security protocols to protect employees' data.

- Safeguard the privacy and security of your employees' biometric information.

- Develop response protocols in the event of a data breach to comply with notice requirements under applicable laws.

- Obtain written consent from employees before collecting any biometric information.

- Never sell biometric data or share with third parties unless you are doing so with the consent of the subject and in compliance with applicable law.

- Review agreements with service providers to ensure compliance with your own biometric data policy and to properly allocate risk in your contracts.

- Consult counsel for help in reviewing your workplace's use of biometric data for compliance with applicable law.

Notes

[1] 740 Ill. Comp. Stat. Ann. 14/15.

[2] 740 Ill. Comp. Stat. Ann. 14/10.

[3] 740 Ill. Comp. Stat. Ann. 14/20.

[4] Tex. Bus. & Com. Code Ann. § 503.001.

[5] Rev. Code Wash. Ann. 19.375.010 et seq.

[6] H.B. 72, 30th Legislature, Reg. Session (Alaska 2017).

[7] H.B. 5019, 99th Legislature, Reg. Session (Mich. 2017).

[8] H.B. 518, 65th Legislature, Reg. Session (Mont. 2017).

[9] H.B. 523, 2017 N.H. H.R., Reg. Sess. (N.H. 2017).

[10] See, e.g., Connecticut (Conn. Gen. Stat. § 36a-701b); Massachusetts (Proposed H.B. 225, 2015).

Robert T. Quackenboss *is a partner and* ***Madalyn K. Doucet*** *is an associate in the Washington, DC office of Hunton Andrews Kurth LLP. Bob litigates complex employment, labor and business disputes He can be reached at (202) 955-1950 or rquackenboss@HuntonAK.com. Maddie represents employers in all phases of the employment relationship, advising clients on compliance with federal and state laws and representing them in labor and employment disputes. She can be reached at (202) 955-1577 or mdoucet@HuntonAK.com.*