LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

THURSDAY, MAY 18, 2023

PERSPECTIVE

Are biometric data violation cases coming to a courthouse near you?

By Arthur F. Silbergeld and Aya Z. Elalami

While Texas, Illinois, and Washington are currently the only states with dedicated biometric privacy laws, many states have expanded their comprehensive privacy laws, placing greater restrictions on the collection, use, and sharing of biometric information.

As the use of biometric technology becomes more prevalent in our day-to-day life, there has been an influx in statutes and litigations focused on the privacy and security of collecting and sharing biometric information. Biometric Information includes body measurements and calculations related to human characteristics, including retina scans, fingerprints, voiceprints, hand scans, or face geometry. Depending on the circumstances, such information can be used for very practical purposes or for politically malicious ends. Unlike passwords or credit card numbers, biometric data cannot be changed or canceled, leaving the individual permanently vulnerable to invasion of privacy, misuse of personal information, and impersonation.

When biometric information is compromised or stolen, companies face serious repercussions, such as identity theft and data breaches. For example, in 2017 Equifax announced a data breach that exposed the personal information of 147 million people, and in 2021 T-Mobile experienced a cyberattack exposing millions of customers' personal information. As a result, both companies entered into multi-million dollar settlements.

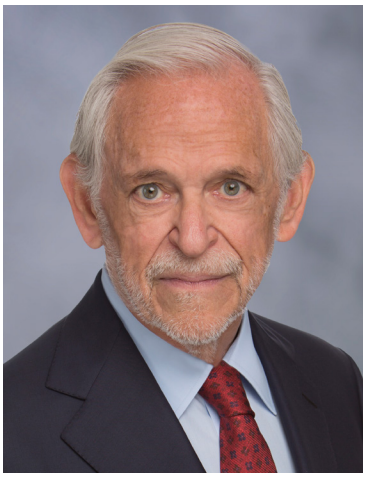
Because of concerns surrounding biometric information, several states have already imposed dedicated biometric privacy laws or comprehensive privacy laws, which if not followed, can expose a company to billions of dollars in liability. For employers who use biometric fingerprinting to track attendance at work and working time, the consequences can be serious.

States such as Illinois, Texas, and Washington have passed laws regulating the collection and storage of biometric data. The Illinois Biometric Information Privacy Act (BIPA) is the most comprehensive biometric privacy law in the United States and was the nation's first legislative control placed on the collection and use of personally identifiable biometric data. Under BIPA, an entity is prohibited from collecting and disclosing an individual's biometric data unless that individual has given prior consent to the collection and disclosure. Failure to comply will result in significant statutory damages – $1,000 per negligent violation of the statute and $5,000 per intentional or reckless violation.

Until recently, BIPA failed to address the issue of whether a claim occurs only once when the first scan or first transmission occurs or if such a violation is deemed to occur each time an entity scans or transmits biometric information. The Illinois Supreme Court recently clarified this in a 4-3 decision, finding in the context of employment that a separate violation occurs each time a private entity scans or transmits a person's biometric identifier without consent. In *Cothron v. White Castle Systems*, the defendant implemented a system that required employees to scan their fingerprints to access their computers and pay stubs. 2023 IL 128004 (Feb. 17, 2023). The biometric information would then be transmitted to a third-party payroll processor that would authenticate each fingerprint scan. The Court held that White Castle violated BIPA by failing to seek employees' consent regarding the collection and dissemination of their biometric information. Although White Castle argued that the injury occurred only once when the first scan or transmission occurred because any subsequent scan would not provide White Castle with additional information, the Court disagreed, finding instead that a violation occurs each time White Castle scanned a person's biometric information or disseminated the information. The Court's reasoning was that the fingerprint scan system requires a person to re-disclose his or her fingerprint to the system so that the print may be compared with the stored copy, and this happens each time a person uses the system. The Court noted that as a result of this decision, White Castle's damages could reach ridiculous heights, exceeding $17 billion.

Remarkably, consumers do not have to demonstrate an injury or adverse effect as result of a BIPA violation. For liability to arise, consumers only need to show that a company collected their personal data without prior consent or failed to inform them how the information would be used. Given the significant penalties businesses may be exposed to when violating BIPA, it is vital to take the necessary precautions to limit their liability. There are five specific steps organizations should consider to avoid potential liability when constitutional or statutory privacy rights impact the collection and sharing of biometric information:

Arthur F. Silbergeld *is an employment law partner, and* **Aya Z. Elalami** *is an associate at Thompson Coburn LLP.*



1) Provide notice
Organizations must provide notice to individuals before collecting their biometric information. The notice must be written and disclose the data that is being collected or stored, the purpose of the collection, and the length of time the information will be stored.

2) Obtain written consent
Organizations must obtain written consent from individuals before collecting their biometric information. The written release must have "informed written consent" or, in the employment context, be "executed by an employee as a condition of employment." Entities need only to obtain consent which covers subsequent collection and disclosure in advance of the first use and not in advance of each use.

3) Written policy and retention schedules
BIPA requires private entities that "possess" biometric data to develop a written policy establishing a retention schedule and guidelines for destruction of biometric data. Destruction of biometric data can occur either once the original purpose of the retention has been exhausted or three years after an employee's last interaction with the employer (whichever comes first).

4) Not disclose to a third party
The biometric information must NOT be disclosed to a third party unless: (1) the employer obtains consent for disclosure, (2) the disclosure completes a financial transaction requested by the employee, or (3) the disclosure is required by law through a valid warrant, subpoena, or otherwise. Additionally, private entities in possession of biometric data are prohibited from selling the data.

5) Reasonable standard of care
An employer must use a "reasonable standard of care" in storing, transmitting, and protecting biometric data. This standard is relative to industry precedent and must be at least as protective as "how the company stores, transmits and protects other confidential and sensitive information."

While Texas, Illinois, and Washington are currently the only states with dedicated biometric privacy laws, many states have expanded their comprehensive privacy laws, placing greater restrictions on the collection, use, and sharing of biometric information. For example, while the California Constitution contains a general protection of the right to privacy (Cal. Const. art. I, § 1), the State recently expanded its Privacy Rights Act (CRPA) to include certain types of biometric information as "sensitive personal information" and provide consumers the right to limit businesses' use of that information. Cal. Civ. Code § 1798.100 et seq. Further, states such as Alaska, Montana, Massachusetts, New Hampshire, and Oregon have introduced legislation regarding the handling of biometric information.

Due to the overwhelming concerns surrounding the security and privacy of biometric information, it is only a matter of time before more states impose specific, strict biometric privacy laws which require compliance and could expose employers to substantial monetary sanctions. Employers should stay up-to-date with the latest biometric privacy regulations decisions and follow best practices to limit their exposure to possible penalties.