Published on *The National Law Review* https://natlawreview.com

To Scan or Not to Scan: Surge in Lawsuits under Illinois Biometrics Law

Article By:

Michael G. Morgan

Mark E. Schreiber

In Depth

The Illinois Biometric Information Privacy Act (BIPA) is having its moment. At least 32 class action lawsuits have been filed by Illinois residents in state court in the past two months challenging the collection, use and storage of biometric data by companies in the state. This may cause a reassessment of company strategies and development of new defenses in the use of advancing biometric technology.

Although BIPA has been on the books for nearly a decade, the recent surge in lawsuits has likely been brought on by developments in biometric scanning technology and its increased use in the workplace. In the vast majority of these lawsuits, the plaintiffs allege BIPA noncompliance against their employers based on the employers' use of fingerprint-operated timeclocks. Specifically, they claim that the collection, use and storage of fingerprints in this manner violates BIPA's requirement of consent, notice and disclosure.

Components of the Illinois Statute

Illinois enacted BIPA in 2008 in response to the introduction of biometrics across multiple industries. At the time, many large companies were piloting biometric scanning applications in Chicago and elsewhere in Illinois, such as finger-scan technologies for authentication purposes in financial transactions. 740 ILCS 14/5(a). The Illinois legislature voiced concern over the privacy implications of biometrics because, unlike many other types of sensitive information, biometrics are immutable and cannot be changed in the event of a compromise. 740 ILCS 14/5(c).

At its core, BIPA sets out to regulate companies' collection and storage of biometric data by creating a private right of action for consumers and employees. BIPA broadly defines "biometric information" to include "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10. A "biometric identifier" is defined to mean "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. It does not include photographs, digital signatures, writing samples and

biological samples used for screening, which are not protected under the statute. 740 ILCS 14/10.

With the privacy of consumers and employees in mind, BIPA requires that companies be transparent about their practices regarding the collection, use and storage of biometric data. BIPA imposes three requirements:

1. Creating a publicly available written policy that establishes the retention schedule and outlines guidelines for permanently destroying biometric data in the company's possession;

2. Fully informing the data subject and receiving the data subject's written consent prior to collecting or storing the data subject's biometric data; and

3. Protecting the biometric data in its possession using the industry's reasonable standard of care and in the same or more protective manner that the company stores other confidential and sensitive information. 740 ILCS 14/15.

BIPA also prohibits companies from selling, trading, leasing or otherwise profiting from biometric data in its possession. 740 ILCS 14/15(c).

Potential Damages

Failure to comply with BIPA can be costly. Under the statute, each wronged party is entitled to receive actual damages or liquidated damages of $1,000 for each negligent violation and actual damages, or liquidated damages of $5,000 for each intentional or reckless violation. 740 ILCS 14/20. BIPA also provides the prevailing party reasonable lawyers' fees and costs, as well as injunctive relief. 740 ILCS 14/20. These remedies create incentives for the filing of cases, especially class actions where the potential exposure can be massive in instances where large volumes of biometric information are involved.

This potential exposure arises even in situations where the violation appears technical or procedural in nature and does not appear to have caused any tangible loss to any individual. There are multiple legal issues and defenses that arise in this type of case, and will inevitably be the subject of litigation. Nevertheless, and like many privacy-focused statutes, Illinois courts have not yet interpreted BIPA's key components or the requirements for recovering in an individual or class action. Current litigation remains in the early stages. It remains unknown how damages will be calculated or if plaintiffs will be entitled to liquidated damages for alleged technical or procedural violations.

Other States' Biometric Data Laws

Illinois is one of three states with privacy laws pertaining to biometric data; however, it is the only statute of its kind that creates a private right of action for violations of the law. Texas and Washington have similar statutes that regulate the collection, use and storage of biometric data, but both statutes leave enforcement of the law up to their respective Attorneys General. State legislatures in Alaska, Connecticut, Massachusetts and New Hampshire are currently considering similar statutes. If adopted, the statutes in Alaska and New Hampshire would create a private right of action that mirrors BIPA in terms of potential damages for negligent and intentional violations.

Company Strategies

Companies that collect, use or store biometric data of Illinois residents should assess their current policies and practices to ensure they are in compliance with BIPA. Companies should also review their cyber liability and other insurance policies to determine the likelihood of coverage in the event of a lawsuit.

If a claim is brought, it is possible that privacy and/or cyber liability insurance policies may cover the costs related to defending actions brought under BIPA. These claims may be covered under certain types of cyber, wrongful data collection or related policies.

National Law Review, Volume VII, Number 312