Bloomberg Law

The United States Law Week

INSIGHT: Using Retina Scans, Fingerprints in Illinois? Practice Tips to Avoid Class Actions

By Stuart D. Levi, William Ridgway, James Talbot, Daniel Healow, and Brian O'Connor

March 15, 2019

It's now easier for individuals to sue businesses that fail to comply with the Illinois Biometric Privacy Act. Skadden attorneys expect a wave of class actions and offer practice pointers for complying with the law.

The Illinois Biometric Privacy Act requires affirmative consent for businesses to collect biometric markers from their customers or employees, including fingerprints, retina scans, and facial geometry scans, which could include identifying individuals through photographs.

Illinois was the first to regulate biometric data usage, but other states are poised to adopt similar legislation, and Washington and Texas already have regulations on the books.

BIPA, however, remains the only regime that allows private individuals to bring a lawsuit and recover statutory damages of up to $5,000 per violation with no cap on aggregate damages.

In its recent unanimous ruling, the Illinois Supreme Court held that plaintiffs need not suffer harm other than a violation of the law in order to bring a lawsuit.

Exposure to Liability

As a result, failing to follow BIPA's procedures exposes businesses to liability even without an allegation that the procedural violation caused additional harm to an individual. As other states pass similar laws in order to fill the federal void, they may decide to clearly resolve the issue in the text of their laws.

This decision leaves other important questions unresolved. Courts continue to grapple with which injuries are "concrete" enough to give individuals Article III standing to bring a lawsuit.

In a recent case dealing with a challenge to the "face grouping" feature in Google Photos (which scans photos to create face templates for different individuals), the U.S. District Court for the Northern District of Illinois concluded that retaining and collecting face templates without authorization was not enough for standing. The court stressed that, even if users were unaware that Google was obtaining biometric data from their photos, there was no evidence that this practice created a substantial risk of harm because Google had not leaked or disclosed the data to third parties.

In another recent decision from the same judge, the court likewise held that an employer's retention of fingerprints and handprints without consent and disclosure under BIPA was not itself a concrete injury that conferred standing.

BIPA Compliance Practice Pointers

As a threshold matter, businesses must assess whether BIPA covers their operations. As of now, the statute applies to retina or iris scans, fingerprints, voiceprints, and scans of hand or face geometry. Many businesses use systems requiring employees to scan their fingerprints, and the law may also cover less obvious technologies. Past cases have challenged features such as photo-tagging in social media applications and video game avatars based on user face scans.

BIPA is a complicated statute that comes with several legal pitfalls, so a careful review of its terms is critical. As a starting point, the following measures should help reduce the risk of a BIPA class action:

1. Define the business need for biometric data. Many of BIPA's requirements are tied to the purpose of the collection or retention of biometric data. For example, one must destroy biometric data within three years of an individual's last interaction with the business, or as soon as the purpose for the collection of that person's biometric data is satisfied, whichever is earlier.

Thus, businesses should document the purpose for any biometric data collection and provide detailed written policies to employees and customers that spell out why and how the data will be collected, stored, retained, used, and destroyed.

2. Implement a security protocol to protect the data. BIPA requires businesses to protect biometric data using a reasonable standard of care within their industry that is at least as protective as the manner in which the entity protects its most confidential and sensitive information. Apart from the statutory requirements, recent decisions on Article III standing underscore the importance of avoiding a breach involving biometric data.

Strong cybersecurity thus serves as an important safeguard against BIPA litigation exposure.

3. Guard against improper data transfers. Unless disclosure is required by law, businesses are prohibited from sharing biometric information with a third party without the individual's prior consent, including with vendors and service providers.

Indeed, plaintiffs have succeed in establishing Article III standing by alleging that biometric data was shared with a third party, such as a biometric timeclock vendor, so any data transfer must be carefully evaluated.

4. Ensure vendor compliance. Even if biometric data is properly transferred to a vendor, businesses should review vendor contracts (including indemnification provisions and insurance requirements) and include provisions (e.g., for data storage) that require vendors to adhere to the law and report any data breaches.

5. Consider arbitration and class action waivers. Consumer and employee arbitration agreements and class action waivers, if appropriate, may limit BIPA liability exposure, particularly because Illinois is a jurisdiction that has been willing to enforce such agreements.

Given the Illinois Supreme Court's ruling, and the prospect of new biometric data regulations from other states, businesses must proceed with caution when it comes to biometric data or face the prospect of costly class action litigation.

Author Information

Stuart D. Levi is a partner at Skadden in New York. He is co-head of Skadden's Intellectual Property and Technology Group, and he coordinates the firm's blockchain, outsourcing and privacy practices.

William Ridgway is a partner at Skadden in Chicago. A former federal prosecutor and experienced trial and appellate lawyer, he focuses on cybersecurity and data privacy matters, white collar crime, and intellectual property litigation.

James Talbot is counsel at Skadden in New York. He focuses on transactional matters, including complex technology development and licensing, intellectual property matters relating to mergers and acquisitions, outsourcing of business practices, information security and privacy projects, as well as internet domain name matters.

Daniel Healow is an IP & technology associate in Skadden's Palo Alto, Calif., office.

Brian O'Connor is a litigation associate in Skadden's Chicago office.