Illinois Supreme Court Holds That Biometric Privacy Law Does Not Require Actual Harm for Private Suits

01 / 29 / 19

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Daniel Healow
Associate / Palo Alto
650.470.3168
daniel.healow@skadden.com

Brian O'Connor
Associate / Chicago
312.407.0514
brian.oconnor@skadden.com

Four Times Square
New York, NY 10036
212.735.3000

The Illinois Supreme Court ruled that an Illinois biometric privacy law does not require individuals to show they suffered harm other than a violation of the law in order to bring suit. As a result, entities are at a greater risk of liability for failure to follow legally required procedures for handling biometric information collected or stored in Illinois.

Background

The Illinois Biometric Privacy Act (BIPA) is a uniquely expansive state law that imposes requirements on businesses that collect or otherwise obtain biometric information, including fingerprints, retina scans and facial geometry scans (which could include identifying individuals through photographs).[1] Among other requirements, businesses must receive written consent from individuals before obtaining their biometric data, and they must disclose their policies for usage and retention. Though Illinois was the first state to pass a law specifically regulating biometric data usage, other states are currently considering the issue, and Washington and Texas have already passed similar legislation. BIPA, however, is currently the only state law that allows private individuals to bring suit and recover damages for violations. For negligent violations, individuals can recover the greater of $1,000 or their actual losses. For reckless violations, the baseline award increases to $5,000.

In this class action, *Rosenbach v. Six Flags Entertainment Corp*., plaintiff Stacy Rosenbach argued that Six Flags violated BIPA when it required her son to scan his fingerprint in order to use a season pass. Rosenbach alleged that Six flags never informed her about the fingerprint requirement when she bought the pass, and they never provided a policy detailing how they would use or store the information. She did not claim that these violations of the law caused her any additional harm, financial or otherwise. BIPA allows "aggrieved" individuals to bring suit when an entity violates the requirements for handling their biometric data, and the parties disputed who qualifies as "aggrieved."

The Decision

On January 25, 2019, the Illinois Supreme Court held that private individuals may bring suit even if the only harm was a violation of their legal rights.[2] The court decided that anyone whose rights under BIPA were violated qualifies as "aggrieved," and rejected the argument that the violation needs to cause some type of additional harm. Since the Illinois legislature did not define "aggrieved," the court reasoned that the word should have its ordinary meaning, which has traditionally included the denial of a legal right. By passing BIPA, the Illinois legislature decided that individuals have rights of privacy and control over their biometric data. Thus, when an individual's BIPA rights are violated, they are "aggrieved" within that word's ordinary meaning.

The *Six Flags* decision clarifies who is allowed to bring a lawsuit for violations of BIPA. 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.[3]

Unresolved Issues

This decision leaves other important questions unresolved. In particular, courts have grappled with the question of which types of injuries are sufficiently "concrete" to give individuals constitutional standing to bring suit in federal court. In a recent ruling from

[1] The text of the BIPA can be found here.

[2] The decision is available online here.

[3] Federal agencies such as the FTC may be increasingly focused on instances of actual consumer harm.

a U.S. District Court in Illinois, the court emphasized that a technical violation of BIPA would not always be enough.[4] There, the court dealt with a challenge to the "face grouping" feature in Google Photos, which automatically scans photos to create face templates for different individuals. The court held that neither the retention nor the collection of face templates without authorization was a concrete injury. The court emphasized that, even assuming that users did not know 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 this information to third parties.

Other courts have come to different conclusions. Last year, a U.S. District Court in California held that Facebook users had standing to challenge Facebook's facial recognition feature, even though the only harm they alleged was a violation of their rights under BIPA.[5] The court relied on the Illinois legislature's finding that since biometric information cannot be changed, it presents heightened risks associated with identity theft. These divergent outcomes illustrate the range of approaches courts are taking in suits addressing technological harms. Some courts defer to legislative attempts at addressing perceived risks, while others require parties to show harms that can be analogized to traditional injuries.

For businesses that find themselves on the receiving end of a lawsuit under BIPA, there are other lines of defense that have not yet been resolved by courts. Some businesses may argue that individuals have effectively consented to the use of their data by taking actions such as placing their hand on a fingerprint scanner. As a result, they may not have suffered an injury sufficient for constitutional standing. In the case of facial recognition, however, courts have been skeptical of this argument. Individuals may not know that by uploading a photo, they are subjecting it to facial geometry analysis.

Key Takeaways

Under Illinois law, failing to follow proper procedures for handling biometric information can expose businesses to liability, regardless of whether anyone is directly harmed in the process. As other states pass similar laws, this may vary on a state-by-state basis. Furthermore, courts remain divided on whether a violation of BIPA necessarily causes a concrete injury that confers constitutional standing.

In light of the emerging patchwork of state laws, businesses should undertake a careful state-by-state analysis before embarking on a biometric data collection effort. For example, under Texas law, voiceprint data used by financial institutions is not subject to the state's biometric identifier law, whereas in Washington, certain financial institutions are entirely exempt from any of the state's biometric data restrictions. These variances could create enough operational difficulty and expense that using nonbiometric alternatives may be the best option for many businesses.

BIPA Compliance Practice Pointers

When businesses use biometric data in Illinois, they should ensure that their practices comply with BIPA. As of now, BIPA 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. Note, however, that BIPA removes certain types of data from its reach, including "information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment or operations under [HIPAA]." As a result, businesses should carefully consider each exception to determine their obligations.

Additionally, businesses should evaluate their business needs *before* collecting data. Businesses can reduce long-term compliance costs by taking the following considerations into account:

1. **Duration.** At most, an entity can retain information for the lesser of: (i) fulfillment of the purpose or (ii) three years after last contact with the data subject, whichever comes first. Thus, a narrow purpose may limit an entity's ability to retain useful biometric information for the needed duration.
2. **Scope.** If the scope of the purpose is too narrow at the outset for a later use, the business must obtain additional consent prior to undertaking that use, resulting in unnecessary delay and expense.
3. **Transferability.** Unless disclosure is required by law, covered entities are prohibited from sharing biometric information with a third party without the individual's prior consent, including with vendors and service providers.

[4] The decision is available online here.

[5] The decision is available online here.