



News & Types: Client Advisories

# Risks and Compliance Under the Illinois Biometric Information Privacy Act: No Actual Harm Required for Private Cause of Action

10/23/2020

Practices: Intellectual Property & Technology

## EXECUTIVE SUMMARY

Recent rulings from the Illinois Supreme Court and the Seventh and Ninth Circuit Courts of Appeals that actual harm is not required to establish a cause of action for a violation of Illinois's Biometric Information Privacy Act ("BIPA"), together with Facebook's agreement to settle BIPA class action claims for \$650 million, have reaffirmed that businesses that choose not to comply with BIPA's requirements do so at their peril. Businesses that anticipate coming into contact with biometric identifiers or biometric information of Illinois residents should review their biometric data collection and handling policies and practices, and take appropriate action to ensure that they are in full compliance with BIPA's requirements.

Recent news of Facebook, Inc. agreeing to pay \$650 million to settle a class action lawsuit for allegedly collecting users' biometric data in violation of Illinois's Biometric Information Privacy Act (740 ILCS 14/1 et seq.) ("BIPA") demonstrates the unique and serious risks BIPA presents to businesses that collect and use biometric information. The Facebook settlement involves claims brought on behalf of Illinois residents whose pictures were uploaded to Facebook, from which Facebook allegedly scanned and stored users' biometric data for use with Facebook's "Tag Suggestions" feature and other features involving facial recognition technology. As the only biometric information privacy law in the United States to provide for a private cause of action, BIPA enables "aggrieved" plaintiffs to claim actual damages or statutory damages (\$1,000 for each negligent violation or \$5,000 for each intentional or reckless violation), in addition to reasonable attorneys' fees and costs and injunctive relief. 740 ILCS 14/20. Decisions from the Illinois Supreme Court and the U.S. Courts of Appeals for the Seventh and Ninth Circuits in the past two years have further strengthened plaintiffs' ability to allege claims under BIPA, making it more important than ever for businesses to understand BIPA's requirements and take action to comply.

BIPA concerns businesses and other "private entities" that contemplate collecting and/or utilizing biometric identifiers and biometric information of employees or customers located in Illinois, such as fingerprint scanning

for employee timekeeping or “season pass” customer verification purposes. BIPA defines “biometric identifiers” as an individual’s retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, and “biometric information” means any information based on an individual’s biometric identifier that is used to identify an individual. 740 ILCS 14/10. Two key provisions of BIPA concern what steps a business must take before collecting or obtaining biometric identifiers and information. Section 15(a) of BIPA requires a business to make available to the public a written policy detailing its retention schedule and guidelines for permanently destroying biometric identifiers and information. 740 ILCS 14/15(a). Section 15(b) requires a business to obtain prior written consent before collecting or obtaining an individual’s biometric identifier or information. 740 ILCS 14/15(b).

As mentioned above, BIPA allows plaintiffs “aggrieved” by an alleged violation to claim actual or statutory damages. Several major state and federal appellate cases have found that a “technical” BIPA violation without evidence of actual harm still enables a plaintiff to claim statutory damages under BIPA. The Illinois Supreme Court ruled in January 2019 in the *Rosenbach v. Six Flags Entertainment Corp.* case (2019 IL 123186) that a plaintiff is not required to suffer actual harm to have a cause of action for a BIPA violation, thereby resolving the conflict among Illinois courts whether a “technical violation” of BIPA’s requirements without actual harm could give a plaintiff the ability to sue a non-compliant business as an “aggrieved” party.

Among federal courts, whether a mere technical BIPA violation could confer standing to sue in federal court under Article III of the U.S. Constitution has given rise to a circuit split. The Ninth Circuit in *Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019) found that violations of BIPA Sections 15(a) and 15(b), even without actual harm, violated the plaintiffs’ common law right to privacy and therefore satisfied federal Article III standing requirements. The Seventh Circuit in *Bryant v. Compass Group U.S.A., Inc.*, No. 20-1443 (7th Cir. 2020) similarly found that a violation of BIPA Section 15(b), but not Section 15(a), leads to an invasion of personal rights that, per the U.S. Supreme Court’s decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), creates a concrete and particularized injury sufficient to grant Article III standing to a plaintiff. These approaches are in contrast to the Second Circuit’s finding in *Santana v. Take-Two Interactive Software, Inc.*, 717 F. App’x 12 (2d Cir. 2017) that, because the plaintiff had given apparent consent by agreeing to sit for his face to be scanned to be digitally inserted into a video game, a bare procedural violation of BIPA’s requirements did not lead to an injury rising to the level of Article III standing.

As the Facebook settlement has demonstrated, businesses that choose not to comply with state biometric information protection statutes such as BIPA do so at their peril. In light of the decisions of the Illinois Supreme Court and the Seventh and Ninth Circuits affirming plaintiffs’ rights to sue for violations of BIPA without evidence of actual harm, businesses that anticipate coming into any type of contact with biometric identifiers or biometric information of Illinois residents should first conduct a careful review of their biometric data collection and handling policies and practices, and take appropriate action to ensure that they are in full compliance with BIPA’s requirements.

For additional information about BIPA compliance, please contact Kenton Knop or any other member of Masuda Funai’s Intellectual Property & Technology Practice Group.