WINSTON & STRAWN LLP

CLIENT ALERT

Biometric Privacy Litigation: The Next Class Action Battleground

NOVEMBER 2, 2017

In the past year, the class action plaintiffs' bar has discovered a new statutory tool, complete with a large pool of potential plaintiffs, high statutory damages, and a private right of action: the Illinois Biometric Information Privacy Act (BIPA). Although BIPA was enacted in 2008, litigation under the statute began in earnest in 2015, with several high-profile suits against social media websites alleging improper collection of facial geometries in photographs without notice and consent. Since that time, over 40 class action complaints have been filed, vaulting BIPA into the spotlight alongside the Telephone Consumer Protection Act (TCPA) as one of the hottest class action trends. Notably, these claims are being brought against companies in various industries, essentially targeting companies that employ Illinois residents.

BIPA litigation is spurred on by a private right of action that allows plaintiffs to seek $1,000 for each "negligent" violation of the act, or $5,000 for each "intentional or reckless" violation, plus attorneys' fees. While the scope of an "intentional violation" is untested, plaintiffs are seeking huge damages by claiming that each use of biometric information by an organization (*e.g.*, each swipe of a fingerprint to clock an employee in or out) constitutes a separate intentional violation of the law.

Notice and Consent Under BIPA

Generally, BIPA regulates, but does not forbid, the collection and use of biometrics. The law defines biometric identifiers as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." To collect or use biometrics, an entity must first: 1) provide written notice to individuals that the collection will occur as well as the purpose and length of the collection; and 2) receive informed written consent from the individual to proceed with the collection. In addition, an entity must first obtain additional consent before sharing an individual's biometric information with a third party.

BIPA Litigation

To date, class action plaintiffs have focused on allegations that organizations failed to comply with BIPA's notice and consent mandates. Two types of fact patterns have emerged: 1) improper use of facial recognition technology; and 2)

improper collection and use of fingerprints, primarily in the employment context. Early facial recognition decisions indicate that courts are willing to interpret BIPA's definition of "biometric data" to include facial geometries collected from scanned photographs, as opposed to direct scans of a person's face. Similarly, dozens of complaints have been filed alleging that companies failed to provide notice or obtain consent before collecting individuals' fingerprints. This complaint typically arises in the employment context, where hourly employees use their fingerprints to clock in.

Litigation Defenses and Responses

While most of the litigation in this space is still in its fledgling stages, several common defenses have already arisen, with varying degrees of success. First, as noted above, the scope of what is considered a "biometric identifier" is largely untested and, especially in the facial recognition context, several defendants have argued that the information at issue falls outside of BIPA.

Second, and more successfully, defendants argue that the "harm" suffered by the plaintiffs is too abstract or immaterial to give rise to standing under the Supreme Court's ruling in *Spokeo v. Robins*. In that ruling, the Court held that Article III standing requires a concrete injury even in the context of a statutory violation. In several instances, courts have found that technical violations of BIPA do not give rise to standing without evidence of actual harm. However, more recently in *Monroy v. Shutterfly Inc.*, No. 16-cv-10984 (N.D. Ill. Sept. 15, 2017), the District Court for the Northern District of Illinois held that the mere invasion of privacy associated with the defendant's collection of biometric information without the plaintiffs' knowledge or consent was sufficient injury-in-fact to give rise to standing.

As these contradicting decisions indicate, there is significant disagreement among the courts regarding how to interpret *Spokeo* in the privacy context. Similar arguments in ligation relating to data breaches have caused a circuit split that may be taken up by the Supreme Court in the near future, as a writ for certiorari was recently filed for the D.C. Circuit Court of Appeal's decision in *Attias v. CareFirst*.

Finally, despite being an Illinois law, the plaintiffs' bar has been aggressive in pursuing organizations based outside of Illinois, or with only minimal operations in the state. This has naturally given rise to disputes over personal jurisdiction.

Complying with BIPA

So, what should companies do to comply with BIPA to ride out this surge of litigation? There are four key requirements under BIPA for any organization that is collecting, using, or sharing information that could be considered a "biometric identifier":

1. Implement appropriate measures to provide the requisite notice and obtain informed written consent. This includes ensuring that additional consent is obtained when sharing biometric information with a third party.

2. Publish a public privacy policy that outlines the organization's policy for collecting, storing, and disposing of biometric information.

3. Do not "sell, lease, trade, or otherwise profit" from an individual's biometric information. The scope of this prohibition has yet to be tested, and advice from counsel should be sought before sharing biometric information with third parties.

4. Ensure that biometric information is adequately protected. Organizations should be using industry-standard data security practices to protect personal information under state and federal privacy laws and regulations.

Outside of BIPA: Other Laws Governing Biometrics

While biometric class action litigation remains focused on BIPA, several other laws and regulations also govern the collection, storage, and use of biometrics. Initially, both Texas and Washington have statutes similar to BIPA, but without a private right of action. An additional seven state legislatures are also considering similar laws, but whether these laws will contain a private right of action remains to be seen. Moreover, a handful of state breach notification laws include “biometric information” within the definition of “personal information” requiring notification in the event of a breach. In the European Union, biometric information will be governed by the GDPR upon its implementation in May 2018. Finally, at the federal level, the FTC, EEOC, and NTIA have all issued guidelines regarding the appropriate collection and use of biometrics. As these laws continue to evolve, we can expect creative plaintiffs’ lawyers to pursue additional and varied approaches for attempting to bring class actions against companies that use biometric information.

4 Min Read

Related Locations

Charlotte | Chicago | Dallas | Houston | Los Angeles | New York | San Francisco | Silicon Valley | Washington, DC

Related Topics

Class Action Litigation | Biometrics | Privacy Class Actions | Telephone Consumer Protection Act

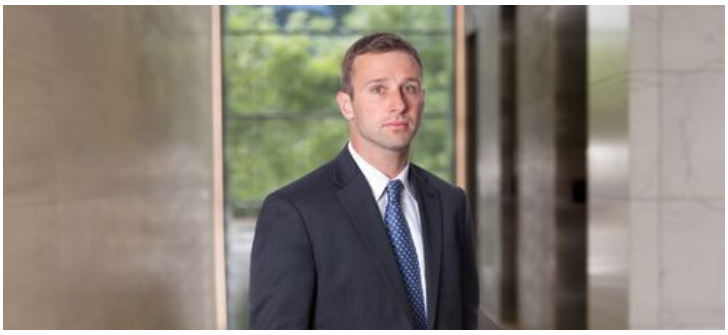
Related Capabilities

Labor & Employment | Privacy & Data Security | Class Actions & Group Litigation | Litigation/Trials | Privacy: Regulated Personal Information (RPI)

Related Regions

North America

Related Professionals



Steven Grimes

Eric Shinabarger