LOEB & LOEB LLP

# Privacy


MARCH 2018

## New Biometric Information Privacy Cases Reveal Breadth of Potential Exposure for Companies

### Illinois BIPA Private Right of Action Spurs Litigation Against a Wide Range of Companies

With the enactment of its groundbreaking Biometric Information Privacy Act in 2008, Illinois became the first state to regulate the collection of an individual's biometric information. BIPA requires organizations to give individuals written notice that data is being collected, why it's being collected, and how long it will be used and stored before being destroyed, as well as to obtain written consent before any collection of biometric information can take place. Organizations can be fined $1,000 for each negligent violation of BIPA and $5,000 for every intentional or reckless violation.

Illinois is one of only three states (with Texas and Washington) that have passed laws specifically governing collection and use of biometric data. Several other states, including Alaska, Connecticut, Montana and New Hampshire, have considered their own biometric data legislation, although none has yet been enacted into law. Illinois, however, is the only state that provides individuals with the right to bring a civil suit for statutory damages — a person "aggrieved" by a violation may seek statutory damages of up to $5,000 per violation. In addition, the statute allows for the recovery of attorneys' fees and expert witness fees. This, predictably, has resulted in a surge of class action litigation.

Since August 2017, more than 40 proposed class action complaints have been filed in Cook County alone. Class actions have been filed against companies across a broad range of industries, including social media platforms, global household names like United Airlines and the Hyatt hotel chain, and smaller companies in the hospitality, supermarket, nursing home, trucking, cargo handling and media industries, among others.

These cases generally fall into two categories of class actions: cases alleging improper use of facial recognition technology to collect biometric data, and cases alleging improper collection and use of fingerprints, primarily but not exclusively against employers.

For example, in December 2017, a former employee sued Presence Health Network, a state-wide health care system including 12 hospitals, 27 senior care facilities and six urgent care centers, for scanning employees' fingerprints as part of its time and attendance recordkeeping without first informing employees that their biometric information was being collected and obtaining their written consent.

Many of the complaints point to language in the Illinois legislation that biometric identifiers are unique because, if compromised, they can't be changed like other personal identifiers, such as Social Security numbers. The complaints typically further allege that the use of biometric information puts individuals at increased risk of identity theft, with no options for recourse.

## Key Themes to Consider

**Extraterritorial Application.** BIPA litigation didn't start heating up until 2015, when users began filing a flurry of complaints against social media companies using facial recognition technology to scan and collect biometric data from photographs uploaded to their sites.

One group of cases, which were consolidated and transferred to a federal court in California, could have a significant impact on all BIPA litigation. Currently, a motion for summary judgment is pending on whether BIPA can be applied extraterritorially. The company argues that its use of facial-recognition technology does not violate BIPA, but, even if it did, the biometric data collection process occurs on its servers, which aren't located in Illinois. A ruling in its favor could assist companies with biometric collection system processing conducted outside of Illinois. Arguments on the motion are set for late March.

**Actual Injury Under BIPA.** Whether a plaintiff has alleged actual harm sufficient to support a cause of action continues to be an issue shaping the BIPA landscape, and the decisions have resulted in some, but varying, guidance on the issues.

One of the first cases to address this issue was *Monroy v. Shutterfly Inc.*, a case involving the use of facial recognition technology. In *Monroy*, the court concluded that the invasion of privacy associated with the photo-sharing site's collection of biometric information without the plaintiff's knowledge or consent was sufficient injury-in-fact to give him Article III standing. The district court distinguished its ruling from *McCollough v. Smarte Carte Inc.*, a previous case in the same jurisdiction, wherein the court found that the defendant's improper collection and use of plaintiffs' fingerprints for access to public lockers without prior written consent failed to allege actual and specific injury, and that a mere technical violation of BIPA was insufficient to grant standing without a showing of an actual injury. The *Monroy* court noted that in *McCullough* customers knowingly and voluntarily provided their fingerprints to use the lockers, whereas the photo-sharing platform allegedly collected and stored facial scans without consumers' knowledge or consent. Plaintiffs could therefore credibly allege an "invasion of privacy" in addition to technical violations of BIPA.

Conversely, a New York court found no actual harm from a failure to notify users that a video game uses facial recognition technology to create players' avatars. In *Vigil v. Take-Two Interactive Software, Inc.*, Illinois brother and sister gamers took on New York-based video game maker Take-Two Interactive. The siblings argued that Take-Two's NBA 2K15 game scanned their faces to create personalized basketball player avatars for in-game play without notifying them. A New York federal district court dismissed their claims for lack of Article III standing, concluding that the failure to notify was a procedural issue and didn't cause the plaintiffs any real harm. The Second Circuit affirmed in November, but remanded with instructions to amend the judgment and enter a dismissal without prejudice because the lower court did not have subject matter jurisdiction.

In December 2017, a three-judge panel of the Second District Appellate Court of Illinois, the first Illinois appellate court to address the issue, provided further instructions, opining that while a plaintiff must allege actual harm as a result of the alleged BIPA violation, the harm need not be an economic injury. In *Rosenbach v. Six Flags Entertainment Corp. and Great America LLC*, *the plaintiff* sued the theme park company in 2016 after her son was fingerprinted during the process of buying a season pass for the Great America theme park in Gurnee, Illinois. The plaintiff argued the theme park failed to obtain her son's written consent to be fingerprinted or disclose what it was going to do with the information. And while she admitted that neither she nor her son suffered an actual injury, the plaintiff asserted that she wouldn't have allowed her son to buy the pass if she had known about the theme park's BIPA-related violations.

At the defendants' request, the trial court certified two questions relating to the necessity that the plaintiff incur actual harm: (1) whether a person "aggrieved" by a violation of BIPA must allege "some actual harm," and (2) whether a person can seek liquidated damages or injunctive relief. The appellate court concluded that an actual harm must be claimed, although it doesn't have to be an economic injury. "If a person alleges only a technical violation of the Act without alleging any injury or adverse effect, then he or she is not aggrieved and may not recover under any of the provisions in section 20 [of BIPA]. We note, however, that the injury or adverse effect need not be pecuniary," it said.

In two decisions over the last two weeks, the court in the consolidated social media case in California seemed to expand further this concept, holding that BIPA created a right of privacy in an individual's personal biometric information, and that "[a] violation of the BIPA notice and consent procedures infringes the very privacy rights the Illinois legislature sought to protect by enacting BIPA. That is quintessentially an intangible harm that constitutes a concrete injury in fact."

In a February 26 decision, the court refused to dismiss claims brought by users of the platform, distinguishing both the *McCullough* and *Vigilcases* and recasting the rights under BIPA as "the right to control their biometric information by requiring notice before collection" and "the power to say no by withholding consent." It added, "When an online service simply disregards the Illinois procedures … the right of the individual to maintain her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized. Consequently, the abrogation of the procedural rights mandated by BIPA necessarily amounts to a concrete injury."

In a short, summary opinion in a case involving BIPA claims of non-users, the court concluded that "[t]he fact difference between the cases … does not lead to a different conclusion at this stage." In denying defendant's motion to dismiss March 2, the court noted that defendant's argument that it didn't store face scans of non-users went to the merits of the case and was more properly resolved on summary judgment.

## On the Horizon

As the case law continues to develop, businesses should identify where they may have exposure, review their internal policies regarding collection and use of biometric data, and generally review any of their consumer- or employee-facing documents for the inclusion of such things as notice, class action waivers and disclosures.