Watch for the Expansion of BIPA Claims to New Use Cases and Jurisdictions

By Torsten M. Kracht, Michael J. Mueller, Lisa J. Sotto, and Daniella Sterns*

The Illinois Biometric Information Protection Act is the national engine driving litigation alleging the improper collection and storage of biometric data. The authors of this article discuss two headline grabbing cases and which technologies and jurisdictions are next.

Although several states have enacted or proposed laws protecting individuals' biometric data, Illinois is the only state with an act on the books that currently permits a private cause of action for the unlawful capture and storage of biometric data. Thus, the Illinois Biometric Information Protection Act ("BIPA")[1] is the national engine driving litigation alleging the improper collection and storage of biometric data. Dozens of new putative class cases have been filed under the law in the last six months alone, both inside and outside Illinois, with class lawyers lured by visions of penalties ranging from $5,000 for each willful violation and $1,000 for each negligent violation.[2]

HEADLINE-GRABBING BIPA CASES

The most headline-grabbing cases under BIPA were waged early on against tech giants Shutterfly, SnapChat, Google, and Facebook for their purportedly unauthorized application of facial-recognition technologies to static photos, but the majority of cases have been filed against companies that use ubiquitous fingerprint-capture technology in connection with access control and employee time-keeping systems. For example, grocery retailer Marianos, health club operator Life Time Fitness, Four Seasons Hotels, and United Airlines have all been sued for collecting employee fingerprints to track work hours. Restaurant operator Superossa Restaurant Group has been sued for using fingerprint scans to track cash register use, and tanning salon operator LA Tan and

* Torsten M. Kracht (tkracht@hunton.com) is a partner at Hunton & Williams LLP representing clients from the United States and abroad in complex commercial litigation and arbitration. Michael J. Mueller (mmueller@hunton.com) is a partner at the firm handling class actions and other complex cases. Lisa J. Sotto (lsotto@hunton.com) is the managing partner of the firm's New York office and chair of its global privacy and cybersecurity practice. Daniella Sterns (dsterns@hunton.com) is a litigation associate at the firm.

[1] 740 ILCS 14.

[2] Texas (the Texas Statute on the Capture or Use of Biometric Identifier, Tex. Bus. & Com. Code Ann. § 503.001) and Washington (Chapter 299, Laws of 2017 (Wash. 2017)) are the only other states that enacted statutes expressly addressing the collection of biometric information by private businesses. Neither the Texas nor Washington law, however, provides a private course of action.

daycare provider Crème de la Crème have been sued for using fingerprint capture for customer access control.

Although one case reportedly settled for $1.5 million in late 2016 and others[3] have been dismissed for lack of standing, most private claims under the law are relatively new and there is not a good track record yet of success or failure on which to accurately assess risk. But, if activity earlier this year in the headline-grabbing cases is any indicator, no silver bullet for eliminating the cases has shown itself yet.

SHUTTERFLY

In September, an Illinois federal judge denied a motion to dismiss the putative class action accusing Shutterfly of violating BIPA by collecting and storing facial recognition data without the plaintiff's consent from pictures uploaded to the Shutterfly website.[4] Shutterfly's motion to dismiss argued that (1) BIPA does not apply to scans of biometric data derived from photographs, (2) application of BIPA to the complaint would give it extraterritorial effect in violation of the Dormant Commerce Clause and (3) the plaintiff failed to allege actual damages resulting from Shutterfly's conduct. The court rejected all three arguments.

First, while recognizing that the statute expressly excludes photographs from the definition of "biometric identifier," the court determined that data obtained from a photograph may nevertheless constitute a "biometric identifier." Second, the court found that although the plaintiff is a resident of Florida, it would be inappropriate to conclude that the lawsuit requires extraterritorial application of BIPA or violates the Dormant Commerce Clause at the motion to dismiss stage given that the complaint alleges that the photo was uploaded to Shutterfly's website from a device located in Illinois by a citizen of Illinois and the circumstances surrounding the claim are not fully known. Lastly, the court held that a showing of actual damages was not necessary to state a claim under BIPA, analogizing to other consumer protection statutes with statutory damages provisions such as the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Truth in Lending Act. In a footnote, the court also found that the plaintiff sufficiently alleged an injury-in-fact for Article III and *Spokeo, Inc. v. Robins*[5] purposes by alleging a violation of his right to privacy.

GOOGLE, INC.

In February 2017, another Illinois federal judge denied a motion to dismiss two complaints brought by individuals who alleged Google captured biometric data from

---

[3] *See McCollough v. Smarte Carte, Inc.,* No. 16 C 03777 (N.D. Ill. Aug. 1, 2016); *Vigil v. Take-Two Interactive Software, Inc.,* No. 15-8211 (S.DN.Y. Jan. 30 (2017).

[4] *Monroy v. Shutterfly, Inc*., No. 16 C 10984 (N.D. Ill. Sept. 15, 2017).

[5] 136 S. Ct. 1540 (2016).

facial scans of images taken with Google Droid devices in Illinois without the plaintiffs' consent in violation of BIPA.[6] And in May 2016, a California federal judge denied a motion to dismiss a putative class action of Illinois residents who alleged Facebook scanned and captured their biometric data from images uploaded to Facebook without their consent in violation of BIPA.[7] Like Shutterfly, both Google and Facebook argued that BIPA does not apply to scans of photographs, and Google also argued that the application of BIPA to the plaintiff's claims would give the statute extraterritorial effect and violate the Dormant Commerce Clause. The courts in both cases rejected these arguments and permitted the cases to move forward.

WHICH TECHNOLOGIES ARE NEXT?

While we will almost certainly see a large number of suits continue along the technology lines of the existing suits (in particular for fingerprint scans used to control access or monitor timekeepers and cashiers), we are also likely to see class cases being filed against companies using more sophisticated methods of biometric capture for other marketing and security purposes without first having obtained proper consent from consumers and users. For example:

- brick-and-mortar operators who use facial recognition to identify and track the movement of shoppers in their stores;
- retailers who use facial recognition to identify returning shoplifters;
- app providers who use fingerprint or facial recognition for secured or streamlined access to their app.

WHICH JURISDICTIONS ARE NEXT?

Although Illinois is the only state that currently permits a private right of action for violations of its biometric data privacy laws, suits under the Illinois law are being filed in many jurisdictions around the country. Additionally, other states have similar laws pending, including

- New Hampshire, H.B. 523, 2017 Sess. (N.H. 2017): This bill provides a private cause of action with statutory damages of $1,000 for negligent violations and $5,000 for reckless or intentional violations.
- Alaska, H.B. 72, 13th Leg., 1st Sess. (Alaska 2017): This bill provides a private cause of action only for intentional violations of the statute. The statutory damages are $1,000 for intentional violations and $5,000 for intentional violations that result in profit or monetary gain.

---

[6] *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

[7] *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016).

- Montana, H.B. 518, 65th Leg., Reg. Sess. (Mont. 2017): This bill provides a private cause of action with statutory damages of $1,000 for purposeful or knowing violations and $5,000 for violations that result in profit or monetary gain. (Note, however, that no action has been taken on the bill since April 28, 2017, and it may have died in Standing Committee.)
- Michigan, H.B. 5019, 2017 Sess. (Mich. 2017): This bill provides a private cause of action with statutory damages of $1,000 for negligent violations and $5,000 for intentional or reckless violations.

Although the Texas and Washington laws mentioned above do not provide private causes of action, they also need to be considered when establishing policies and procedures for complying with biometric data privacy laws. If, for example, a private Illinois action were to succeed at trial or result in a large settlement, the defendant may be a soft target for a follow-on action pursued by a state attorney general.

CONCLUSION

It is crucial that retailers ensure that their policies and procedures regarding the capture, retention and disposal of biometric data comply with the various notice and consent requirements outlined in BIPA as well as the Texas and Washington laws. Retailers should also track the development of similar proposed legislation in other states to ensure the continued lawfulness of such policies and procedures.