

# Client Alert

October 2017

## Facing Privacy Suits About Facial Recognition: BIPA Cases Move Forward As More States Consider Passing Biometric Data Laws

Recent judicial interpretations of the Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14, present potential litigation risks for retailers who employ biometric-capture technology, such as facial recognition, retina scan or fingerprint software. Federal judges in various district courts have allowed BIPA cases to move forward against companies such as Facebook, Google and Shutterfly, and retailers who use biometric data for security, loss prevention or marketing purposes may also become litigation targets as federal judges decline to narrow the statute's applicability and additional states consider passing copycat statutes.

### Biometric Privacy Laws on the Books

Currently, Illinois (BIPA), Texas (the Texas Statute on the Capture or Use of Biometric Identifier, Tex. Bus. & Com. Code Ann. § 503.001) and Washington (H.B. 1493, 2017 Sess. (Wash. 2017)) are the only states that have statutes addressing the collection of biometric information by private businesses. Retailers face significant financial exposure for cases brought as class actions under BIPA—the statute permits statutory damages of \$1,000 for negligent violations and \$5,000 for reckless or intentional violations. The Texas and Washington statutes expose retailers to potential civil penalties through attorney general enforcement actions. Because BIPA is the only one of these laws to provide a private cause of action, it has attracted the most litigation.

### Recent Court Decisions

Most recently, on September 15, 2017, an Illinois federal judge denied a motion to dismiss a 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. *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017). 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*, 136 S. Ct. 1540 (2016) purposes by alleging a violation of his right to privacy.

In February 2017, another Illinois federal judge denied a motion to dismiss two complaints brought by individuals who alleged Google captured biometric data from facial scans of images taken with Google Droid devices in Illinois without the plaintiffs' consent in violation of BIPA. *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088 (N.D. Ill. 2017). 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. *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016). 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.

While it is yet to be seen how courts will handle the merits of these BIPA claims, it is worth considering how the allegations waged by the plaintiffs in recent cases could be directed to retailers who use biometric-capture technology for marketing or for in-store security and loss prevention. Although in-store use of biometric-capture technology would currently pose a threat of consumer litigation only within Illinois, the Facebook, Google and Shutterfly cases indicate that retailers can be sued for capturing or storing the biometric information of individuals accessing retailers' websites from within the state of Illinois.

### **Similar Proposed Legislation**

Below are the states that have proposed biometric privacy legislation similar to BIPA this year:

- 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.
- Connecticut, H.B. 5522, 2017 Sess. (Conn. 2017): There is minimal information available about this bill, but its stated purpose is: "To prohibit retailers from using facial recognition software for marketing purposes."
- 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.
- 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.
- 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.

It is worth noting that an amendment to BIPA has been proposed (H.B. 2411, 100th Gen. Assem., 2017 Sess. (Ill. 2017)), which would prohibit private entities from requiring that an individual provide biometric information as a condition for the provision of goods or services, subject to specific exemptions.

### **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. Hunton & Williams LLP is tracking state legislation on this issue as well as all privacy-related litigation regarding biometric identifiers filed against businesses.

**Authors**

**Torsten M. Kracht**

tkracht@hunton.com

**Michael J. Mueller**

mmueller@hunton.com

**Daniella Sterns\***

dsterns@hunton.com

*\*(Associate \*Not Admitted in DC, Admitted Only in Florida Work Supervised by Michael J. Mueller, a member of the District of Columbia Bar)*

© 2017 Hunton & Williams LLP. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.