

Byline

July 14, 2015

States Writing Biometric-Capture Laws May Look To Illinois

by Torsten M. Kracht and Rachel E. Mossman

Published in Law360



Recent class actions filed against [Facebook](#) and Shutterfly are the first to test an Illinois law that requires consent before biometric information may be captured for commercial purposes. Although the instant cases focus on biometric capture activities in the social-media realm, the cases and Illinois law at issue have ramifications for anybody who employs biometric-capture technology, including those who use it for security or sale-and-marketing purposes.

The Recent Suits

Within the last three months, plaintiffs sued Facebook and Shutterfly for purportedly capturing biometric data in violation of Illinois' Biometric Information Privacy Act, 740 ILCS 14 (West). BIPA requires that before collecting and storing any biometric identifier, defined as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," the subject of collection be informed in writing:

1. that the information is being collected and/or stored,
2. of the specific purpose for collecting and length of time the identifier will be stored, and
3. that the subject of the collection execute a written release before any biometric information is captured.

740 ICLS 14/15(b).

The suits against Facebook all make the same basic allegation: Facebook's tag suggestion feature (which identifies friend's faces in photos and makes it easier for the user to "tag" or link the photo to the friend's profile) captures and stores facial features without first receiving the proper consent in violation of BIPA. *Licata v. Facebook Inc.*, 1:15-cv-04022 (N.D. Ill. May 5, 2015); *Patel v. Facebook Inc.*, 1:15-cv-04265 (N.D. Ill. May 14, 2015); *Pezen v. Facebook Inc.*, 1:15-cv-03484, (N.D. Ill. Apr. 21, 2015). The suits allege that Facebook creates "face templates" of its users by collecting and storing biometric information in the form of "facial geometry." *Licata Complaint* at ¶24; *Patel Complaint* at ¶6; *Pezen Complaint* at ¶2. The plaintiffs allege that Facebook has violated all three requirements under BIPA because it began compiling facial recognition data without first informing the subjects of the collection, it has not complied with the duty to inform subjects of the retention period, nor has it gotten the proper written consent for such collection.

States Writing Biometric-Capture Laws May Look To Illinois
by Torsten M. Kracht and Rachel E. Mossman
Law360 | July 14, 2015

BIPA establishes statutory damages of \$1,000 for negligent violations and \$5,000 for intentional or reckless violations, and, in both cases, permits greater recovery if actual damages exceed the liquidated damages amount. 740 ILCS 14/20. All of the suits against Facebook seek damages on a classwide basis for plaintiffs residing in Illinois whose biometric information has been captured by Facebook. The plaintiffs claim that Facebook intentionally violated the statute and that each class member is therefore entitled to at least \$5,000 in damages. One suit estimates the number of Facebook users in Illinois exceeds seven million, which translates to a damages claim in excess of \$7 billion. Pezen Complaint at 4, n. 1. In addition, Pezen alleges that the class of harmed plaintiffs also includes individuals who are not Facebook users, but whose images have been uploaded by users and then captured and linked to “shadow profiles” by Facebook. *Id.* at ¶26.

The suit against Shutterfly similarly alleges that Shutterfly has violated BIPA by collecting facial biometric information without abiding by the notice and consent requirements in the act. *Norberg v. Shutterfly Inc. and ThisLife LLC*, 1:15-cv-05351, (N.D.Ill. June 16, 2015). Plaintiff Norberg asserts that his pictures were uploaded to Shutterfly by someone else and that Shutterfly “automatically scanned and analyzed” his face and used the information to create a template which was then associated with his name. *Norberg Complaint* at ¶27-31.

Expect Similar Suits Outside the Social Media Space

The risks associated with capturing biometric information for commercial use are not limited to social media. As the rapid evolution of biometric imaging technologies has made them less expensive and more accessible, businesses of all types have started using biometric imaging as part of their physical security protocols and to aid in targeted sales and marketing efforts.

At present, the only states with statutes addressing biometric capture for commercial purposes are Illinois and Texas, and the suits discussed above are the very first attempt to litigate under the Illinois statute. However, several other states have similar legislation pending, and the outcome of the lawsuits against Facebook and Shutterfly, as well as others that are likely to soon follow, may impact the way other states address the emerging privacy issue.

The Texas statute defines biometric identifiers as “a retina or iris scan, fingerprint, voiceprint, or record TX of hand or face geometry.” Capture or Use of Biometric Identifier, Tex. Bus. & Com. Code Ann. § 503.001. Like BIPA, the Texas statute requires that businesses inform and receive consent from individuals before collecting any such information, but does not identify the form the notice and consent must take. *Id.* § 503.001(b). However, the potential for expensive litigation is high since Texas has established a private right of action against any one that violates the act and allows for a substantial recovery, up to \$25,000 for “each violation,” of the statute. *Id.* at § 503.001(d).

Alaska and Washington have similar legislation pending. Under the proposed Alaska statute, collection of biometric identifiers without express, documentable consent would give rise to a private right of action for any intentional violations of the statute. H. B. No. 144, 28th Legislature, 1st Sess. (Alaska 2013). The Washington bill, which has passed in the House and is moving through the Senate, seeks to prevent the capture and/or sale of a biometric identifier for commercial use unless the subject is first informed and consents, but importantly does not establish a private right of action. H. B. No. 1094, 64th Legislature, 2015 Regular Session.

As these statutes gain notoriety through cases like those discussed above, businesses already using these technologies in other states need to keep abreast of new legislation that might affect the legality of their practices, and businesses considering the implementation of these technologies should consult local rules and statutes before implementing biometric imaging.