Published on *The National Law Review* https://natlawreview.com

Six Things You Need to Know Before Collecting Biometric Information

Article By:

David S. Almeida

Laura E. Jehl

Paul A. Werner

1. Illinois and Texas recently enacted laws regulating the collection and use of biometric information (*e*., information based on an individual's biometric identifiers, such as iris scans, fingerprints, voiceprints, or facial geometry) and a number of other states, including New York and California, are considering adopting such statutes. The Illinois Biometric Information Privacy Act ("BIPA") permits private rights of action and provides for statutory damages ranging from $1,000 to $5,000 per violation. The Texas analog, entitled Capture or Use of Biometric Identifier ("CUBI"), is enforceable only by the state attorney general and permits civil penalties up to $25,000 per violation.

2. Under both the BIPA and CUBI, "biometric information" is keyed to "biometric identifiers," which include (i) retina and iris scans, (ii) fingerprints, (iii) voiceprints, (iv) hand geometry and (v) face geometry. While the CUBI applies solely to biometric identifiers captured for "commercial purposes," the BIPA contains no such limitation, and applies broadly to all non-governmental entities.

The BIPA exempts a number of biometric identifiers from the statute, while the CUBI contains no specific exemptions. Specifically, the BIPA exempts: (i) writing samples/signatures, (ii) photographs, (iii) biological samples used for testing, (iv) demographic data, (v) tattoos, (vi) physical characteristics, (vii) information gathered in a healthcare setting, (viii) information used for healthcare treatment, (ix) medical tests conducted to treat a medical condition, and (x) information derived from the above.

3. The BIPA contains six key requirements for any private entity in possession of or collecting biometric data:

> (i) Develop a written policy, available to the public, establishing a retention schedule and guidelines for destruction;
>
> (ii) Destroy biometric data when the initial purpose for obtaining/collecting such data has been fulfilled, or within three years of the person's last interaction with the entity, whichever is

sooner;

(iii) Biometric data cannot be collected or otherwise obtained without prior written consent based on a disclosure to an individual that biometric data is being collected and the length of time for which the data is collected;

(iv) Biometric data cannot be sold;

(v) Biometric data cannot be disclosed unless (a) consent is obtained, (b) disclosure is necessary to complete a financial transactions requested or authorized by the subject, (c) disclosure is required by law or (d) disclosure is required by subpoena; and

(vi) Biometric data must be stored using a reasonable standard of care for the entity's industry and in a manner that is the same or exceeds the standards used to protect other confidential information.

The CUBI contains four key requirements for collecting biometric data:

(i) Biometric data may not be collected absent informed consent;

(ii) Biometric data may not be sold or otherwise disclosed absent (a) consent for purposes of identification in cases of disappearance or death, (b) to complete a financial transaction that the individual requested or authorized or (c) disclosure is required by law or by law enforcement pursuant to a warrant;

(iii) Biometric data must be protected using reasonable care and in a manner that is the same as or exceeds that in which other confidential information is protected; and

(iv) Biometric data must be destroyed no later than (with few exceptions) one year from the date on which the purpose for collecting the data ends.

4. Over the last year, more than a half dozen class action lawsuits have been filed under the BIPA. Google, Shutterfly and a handful of social media companies have each been sued over the alleged use of facial geometry recognition software used for photo tagging. Palm Beach Tan and LA Tan were each sued over the alleged use of fingerprint data to act as a membership card, and Smarte Carte was sued over the alleged use of fingerprint security technology to lock and unlock lockers. Daycare company Crème de la Crème was sued recently over the alleged use of fingerprint technology to ensure the secure pickup of children.

5. Thus far, motions to dismiss BIPA class actions at the pleading stage have been unsuccessful, but a number of arguments remain untested. Google has moved to dismiss its case on the basis that the Dormant Commerce Clause prohibits the application of the BIPA in the context of photo websites. Google argues that companies across the country are effectively required to comply with the BIPA as they cannot determine at the outset whether or not an individual in a given photograph is an Illinois

resident. In addition, the Supreme Court's recent decision in *Spokeo, Inc. v. Robins*calls into question whether individuals have Article III standing to pursue technical BIPA violations (*e*., the absent of a written policy), notwithstanding statutory damages.

6. Expect the growth in BIPA class actions to continue. Not only will use of biometric data by tech and other companies continue to grow as new services and product offerings come online, but the variety of defendants already facing BIPA claims – including the recent lawsuit against the Crème de la Crème daycare company – suggests that plaintiffs' counsel have broadened their focus from the tech industry and may assert claims against employers, childcare facilities, healthcare companies and the financial services industry. Whether it is businesses protecting trade secrets through fingerprint access, childcare facilities using fingerprint technology for secure child pickup, health insurers collecting biometrics outside of the treatment setting or banks using fingerprints for account access, the list of possible defendants is extensive.

Given the threat of staggering statutory damages, companies across all industries cannot afford to ignore laws regulating the use of biometric information. Given the novelty of the issues and the potential for statutory damages, there is sure to be an influx of litigation under such statutes in the coming years. Companies must therefore carefully evaluate the types of biometric information they collect and their policies for use and retention of such data, even if they do not collect it directly.

National Law Review, Volume VI, Number 154