The Battle Over Biometrics

A look at the law in Texas and two other states.

BY JOHN G. BROWNING

In January 2018, as Google debuted the "art selfie" feature on its Google Arts & Culture app—enabling people to find their art lookalikes from over 1,200 museums worldwide—users delighted in the chance to match themselves to a painting or sculpture. All Google users, that is, except those in Illinois and Texas. In those two states, the app was blocked for fear of violating the strict biometrics privacy laws on the books there. But just what do such statutes cover, and as biometrics measures become more commonly used by everyone from banks and credit card companies to employers, will laws like these in Texas and Illinois pave the way for similar privacy legislation?

First, it is important to note that commercial use of biometrics data—measurements of one's physical being—has exploded in recent years. With advances in sensors, software, and readers, it has become simpler than ever to employ such things as fingerprints, facial recognition, retinal or iris scans, voiceprint reading, gait analysis, or even keystroke analysis to identify a person. With its accuracy and ease of use, biometric data is being used as part of the authentication protocol for physical devices (like smart phones), online applications, and telephone calls. Banks, for example, regularly employ voiceprint, using a digitized representation of the sound of a customer's voice to authenticate that account holder when he or she calls a customer service line. In February 2016, Mastercard announced that it would accept "selfies" as passwords, allowing cardholders to access their accounts using their faceprints.

But the use of biometrics for identification presents certain pitfalls as well. Unlike a password or Social Security number, a person's biometric data is unique and immutable, and therefore cannot be changed or replaced. Once compromised, a biometric identifier may be lost, leaving the affected individual at a heightened risk for identity theft. In addition, use of biometrics opens up a whole new level of government surveillance. The FBI is already working on "Next Generation Identification," a program that collects voiceprints, iris scans, and other biometric data to supplement its current fingerprint identification system. Facial recognition technology in particular has been used by law enforcement, the Department of Homeland Security, and the Department of Defense for years.

And with such advantages as well as risks, it only makes sense that the capture and use of biometric data would attract legislative scrutiny. Laws addressing biometrics fall into two categories: laws that specifically involve the collection and use of such data by private actors (like businesses) and governmental entities, and broader privacy laws that happen to include biometric information in their definition of personal information. This article will focus on the first type of laws, and particularly on the three states—to date—that have adopted laws regulating the collection, storage, and use of biometric data: Illinois, Texas, and Washington.

Illinois

Illinois was the first state to address businesses' collection of biometric data with the Biometric Information Privacy Act, or BIPA, in 2008.[1] BIPA sets forth a comprehensive set of rules for companies collecting biometric data, and significantly (unlike its Texas and Washington counterparts) creates a private cause of action for Illinois residents whose biometric data is collected or used in violation of these rules. Essentially, there are five key features of BIPA:

(1) it requires informed consent prior to collection;
(2) it prohibits any profiting off biometric data;
(3) it allows only a limited right to disclose the data;
(4) it sets forth both protection obligations and data retention guidelines for businesses; and
(5) it creates a private cause of action for those harmed by BIPA violations.

As to the first of these features, BIPA mandates that a business must give an individual written notice of the collection of biometric data. This notice must specify the purpose of the collection as well as how long the data will be used or stored. In addition, it must receive the individual's written consent. The content and form of this release, however, are not specified. Are electronic notices and releases satisfactory? Probably so, particularly if the terms and conditions are set forth explicitly, along with an "Accept" or "I consent" button.

The second feature, prohibiting a company from selling or otherwise profiting from the biometric data it collects and/or stores, doesn't have much more to it than what the statute's somewhat vague language provides. The third feature, concerning disclosure, bars a business from disclosing a person's biometric data unless: (1) the person consents; or (2) the disclosure completes a financial transaction that the individual requested; or (3) the disclosure is required by applicable state, federal, or local law; or (4) "the disclosure is required pursuant to a valid warrant or subpoena."

As to the fourth feature, BIPA requires a business to give biometric data the same degree of protection as other sensitive, confidential information in its possession, employing the reasonable standard of care within its given industry. The business may not store such data for more than three years from when the initial purpose of collecting the data was fulfilled, or three years from the affected individual's last interaction with the company (whichever is earlier). In addition, the business must have a written, publicly available retention/destruction policy, and must adhere to this policy. Finally, the fifth feature provides a private cause of action to anyone harmed by a business' violation of BIPA. Per the statute, a prevailing party may recover either actual damages or statutory damages of $1,000 (whichever is greater) for each negligent violation, and $5,000 in statutory damages for each intentional violation (or actual damages, depending on which is greater).

BIPA received little fanfare in the immediate wake of its enactment, but a series of 2015 lawsuits against online platforms Facebook and Shutterfly over their collection, storage, and use of biometric data, specifically faceprints/facial geometry, brought renewed attention to the law and its privacy implications.[2]

Texas

Texas' biometric privacy statute, enacted in 2009, might well be called "BIPA-lite."[3] Like its Illinois counterpart, Texas' law applies to the same kinds of biometric information, although unlike BIPA, it doesn't cover data that is converted into a code or template. Texas' statute only protects biometric identifiers, and doesn't contain a broader "biometric information" provision. Both the Illinois and Texas laws require notice and consent, but unlike BIPA, Texas doesn't require a written release. Like BIPA, Texas' statute prohibits the sale of biometric information, and both have restrictions on how it is stored. Texas and Illinois both require employers to store, transmit, and protect the data using reasonable care and in the same manner as the business treats other confidential information. And although both Illinois and Texas require that businesses destroy biometric data that is no longer needed, Texas puts that duty on a faster timetable. Under Texas' statute, the company must destroy such data within a "reasonable time" that does not exceed one year after the biometric data is no longer needed.[4] Of course, the biggest divergence between the two laws is that Texas does not allow for a private cause of action. Under Texas' statute, the attorney general can sue to enforce the statute and seek up to $25,000 per violation.[5]

Washington

Washington's biometric privacy statute took effect July 23, 2017.[6] Like its counterparts, it covers biometric measurements, but it also defines biometric information more broadly—as any "data generated by automatic measurements of an individual's biological characteristics."[7] Like Texas' law, the Washington statute does not specify that consent must be in writing, nor does it create a private cause of action against violators. Its notice and consent provisions, however, do contain an exception that the others don't, carving out an exemption for biometric data collected and stored by the business for "security purposes." This applies to biometric data being stored for "the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value."[8] And unlike in either Texas or Illinois, under certain limited circumstances or with consent, a business may sell biometric information.[9]

The battle over biometric data continues to rage. Other states have considered legislation similar in many respects to the three laws discussed here, including Alaska, Connecticut, Montana, New Hampshire, and Utah. And lawsuits—particularly class actions—continue to be brought under BIPA. But it is not just tech companies that find themselves in the crosshairs. Since July 2017, more than 25 cases have been filed in state and federal courts in Illinois against video game companies, food product manufacturers, gas stations, and even restaurant chains (Wow Bao was sued over its use of facial scans to verify customer orders at self-service kiosks). And with employers using timekeeping systems and security protocols that use biometric identifiers (such as fingerprints or facial scans), the employer/employee relationship will continue to be a battleground for potential liability. In short, facial recognition technology and other biometric measures will continue to be applied, even if the residents of Texas and Illinois don't get to enjoy the occasional innovation like Google's "art selfie." But businesses and their lawyers will have to navigate an increasingly complex regulatory environment in order to ensure compliance. **TBJ**

Notes

1. Biometric Information Privacy Act, 740 ILCS 14 (2008), *et seq.*
2. *See, e.g., Pezen v. Facebook, Inc.*, 1:15-cv-03484 (N.D. Ill. Apr. 21, 2015); *Licata v. Facebook, Inc.*, 1:15-cv-04022 (N.D. Ill. May 6, 2015); *Patel v. Facebook, Inc.*, 1:15-cv-04265 (N.D. Ill. May 14, 2015); *Gullen v. Facebook, Inc.*, 1:15-cv-07861 (N.D. Ill. Aug. 31, 2015); *Norberg v. Shutterfly, Inc.*, 1:15-cv-05351 (N.D. Ill. June 17, 2015).
3. Tex. Bus. & Com. Code Ann. § 503.001.
4. *Id.* § 503.001(c)(3).
5. *Id.* § 503.001(d).
6. Wash. Rev. Code Ann. § 19.375, *et seq.*
7. *Id.*
8. *Id.*
9. *Id.* at § 19.375.020(3).

JOHN G. BROWNING
is a partner in Passman & Jones in Dallas, where he handles commercial litigation, employment, health care, and personal injury defense matters in state and federal courts. He is an award-winning legal journalist for his syndicated column, "Legally Speaking," and is the author of the Social Media and Litigation Practice Guide *and a forthcoming casebook on social media and the law. He is an adjunct professor at SMU Dedman School of Law.*