Hashed & Salted
A Privacy and Data Security Update
January 2022

The Future of Biometric Data: A Challenging Legal Landscape Forward

Films of the 20th century, including *2001: A Space Odyssey*, *Star Trek* and *The Fifth Element*, foresaw a future where the processing of biometric information would be prevalent and in some cases necessary to civilization. That future is now. We scan our fingerprints to unlock computers and phones, use facial recognition to try on glasses, and have our image captured by cameras in advertisements to feed us personalized offers. However, 20th-century cinema failed to predict the challenging legal landscape of the 21st century and how it impacts daily use of technology that captures biometric information, including in the private sector.

Here's our high-level overview of how state law impacts biometric technology today, and where the law may be headed in the future.

The Legal Landscape

While there is no comprehensive federal law regulating the collection and use of biometric information, nor even a single comprehensive law regulating the processing of personal data, there are a number of state laws that should be considered before collecting or processing biometric data.

Biometric identifiers are biological pieces of information used to identify an individual. The definition espoused by most biometric privacy statutes, including the Illinois Biometric Information Privacy Act (BIPA) and the Texas Capture or Use of Biometric Identifier Act (CUBI), is that biometric identifiers are specifically "retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry."

Illinois's Biometric Information Privacy Act

The leading statute for driving litigation around the processing of biometric information is the Illinois Biometric Information Privacy Act, which applies in circumstances where the biometric data is stored or processed in Illinois or the company is processing biometric data of Illinois residents. Under BIPA, companies are required to receive informed written consent before collecting any biometric information. The consent is valid only if the user is first informed a) that biometric information is being collected or stored; b) the purpose of the collection, use or storage; and c) the length of time the biometric information will be collected, stored or used.

Companies are always prohibited from selling or profiting from biometric information, and are prohibited from sharing biometric information except under certain limited exceptions.

Biometric information must be stored and protected with a reasonable standard of care and in a manner that

Attorney Advertising

is at least as protective as that used for the company's other confidential and sensitive information. Biometric information is only permitted to be retained for as long as necessary to achieve the purpose of collection, or three years, whichever comes first.

BIPA is the only law specific to biometric information that contains a private right of action. (The California Privacy Rights Act, which will take effect on Jan. 1, 2023, treats the processing of biometric information for the purpose of uniquely identifying a consumer as sensitive personal information and subject to certain consumer rights to opt out of processing. The private right of action under the California law is limited to data breaches resulting from a violation of the obligation to maintain reasonable security.) Further, the law provides statutory damages up to $1,000 for each negligent violation, and up to $5,000 for each intentional or reckless violation.

Texas's Capture or Use of Biometric Identifier Act

Texas has enacted its own law prohibiting the capture of biometric information, but only for a commercial purpose. (While "commercial" is not defined, extrapolation from the statute's other clauses suggests that this does not include information captured for security or employment purposes.) Biometric information may only be captured if the business receives consent from the individual prior to capturing the data.

Biometric information may be shared or sold but only in limited circumstances. As with BIPA, biometric information is to be stored and protected with a reasonable standard of care and in a manner that is at least as protective as that used for the company's other confidential and sensitive information. However, the data can only be retained for a year, unless it meets one of the enumerated criteria.

CUBI has no private right of action, and civil penalties for violation of the statute are capped at $25,000 per violation.

Washington's Biometric Identifiers Law

Washington's biometric law is the least stringent of the state laws, as it does not apply to scans of facial or hand geometry, or data generated from digital photographs and audio recordings.

Further, the law limits its focus to enrollment of biometric information—which is defined as capturing a biometric identifier, converting it into a reference template that cannot be reconstructed into the original output image, and storing it in a database that matches the biometric identifier to a specific individual.

Additionally, the law is limited to the enrollment of biometric information for a commercial purpose, which means disclosing the data to a third party for marketing purposes.

Finally, businesses are not required to get affirmative consent prior to enrolling biometric information. Rather, businesses can also enroll biometric information if they first provide notice regarding the collection, or if they provide a method to prevent subsequent disclosure of the data for commercial purposes.

Under Washington's law, businesses must only take reasonable care with the biometric information and retain it only for as long as is reasonably necessary.

The Washington law also does not provide a private right of action, leaving its enforcement to the state attorney general.

Litigation Trends Under BIPA

Most of the litigation surrounding biometric identifiers has come from BIPA, due to its private right of action. For a number of years after BIPA was enacted, there was limited litigation. Then, in 2019 and 2020, the Illinois Supreme Court and the Seventh Circuit Court of Appeals made key holdings regarding standing to bring these types of lawsuits.

In *Rosenbach v. Six Flags Entertainment*, the Illinois Supreme Court held that a plaintiff may be entitled to statutory damages even without an actual injury. This case settled for $36 million in June 2021. Then, in *Bryant v. Compass Group USA, Inc.*, the court held that the plaintiff had constitutional standing (and therefore sufficient concrete harm) to bring a lawsuit when she alleged that the defendants collected biometric fingerprint identifiers and information from her and other Illinois residents without following BIPA's informed written consent procedures. This case settled for $6.8 million in October 2021.

Arguments Regarding Jurisdiction

Plaintiffs have sued companies in their home states, and been successful despite choice-of-law provisions. In those situations, courts have applied Illinois law in order to ensure that the Illinois policy of protecting its citizens' privacy interests in their biometric data survived.

Recent Trends

There has been a wave of litigation related to virtual try-ons, and the use of facial scanning technology, without receiving consent from users to collect biometric data. Recently, Apple was also sued for its use of the Face ID feature in its iPhone—a use that allegedly employs facial recognition technology.

Litigation involving voiceprint technology has also been on the rise. BIPA is not clear as to what constitutes "voiceprint" as opposed to voice data, other than it must be more than a simple voice recording. Recently, suits have been brought against a number of companies that allegedly use voice data for purposes other than identifying individuals (e.g., for recognizing a voice in order to follow a command).

The proliferation of lawsuits demonstrates plaintiffs' willingness to experiment with the scope of BIPA. Statutory damages of $1,000 per violation offer a substantial incentive to bring these types of lawsuits, and business are forced to wrestle with potential next steps. While defendants may ultimately be able to defeat these lawsuits in a motion for summary judgment or a motion to dismiss, the cost of getting to that point may be substantial.

While there is no way to guarantee that a lawsuit will not be filed, businesses seeking to mitigate the risk of litigation should consider the following questions:

- **Are you collecting written consent from users prior to collecting any type of biometric information?** Disclosure should follow BIPA requirements and include how the information will be used and for how long it will be retained. If the information will never be used to identify an individual or will never leave the app or phone, that should be disclosed in the banner or other medium used to obtain consent prior to collection.

- **Have you updated your privacy policy to disclose the same information?** Your policy should inform users specifically what information is collected, how it will be retained and the security measures that will be used to help protect personal information, including any biometric identifiers.

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com
Tanya Forsheit . . . . . tforsheit@loeb.com
Daniela Spencer . . . . . dspencer@loeb.com