Articles + Publications | July 6, 2022

Are You Ready for the BIPA Tsunami? The New Wave of Biometric Statutes

Privacy & Cybersecurity Newsletter

WRITTEN BY

Tara L. Trifon | Brian I. Hays | Brianna L. Dally

The Illinois Biometric Information Privacy Act[1] ("BIPA") has steadily become one of the most important and influential privacy statutes in the United States.[2] Indeed, the collection, use, and storage of the biometric identifiers that are governed by BIPA have become pervasive in our society. Consequently, BIPA requires organizations that collect and store the biometric information of Illinois residents to obtain consent and implement policies and procedures to ensure compliance or face significant statutory penalties of $1,000 per negligent violation and $5,000 intentional violation, plus attorney fees.

The growing number of states that have passed laws similar to BIPA means that this is no longer just an Illinois issue. Some states, like Arkansas and California, have included biometric data in their existing privacy laws.[3] Other states, namely Texas and Washington, have passed standalone biometric data laws modeled, at least in part, on BIPA.[4] These statutes broadly define biometric information to include identifiers such as retina and iris scans, palm prints and fingerprints, voice recognition, and facial-geometry recognition. Some even include gait or scent recognition. Some states have followed Illinois' lead by including a private right of action in their statutes.[5] Others provide that the law can only be enforced by the state's attorneys general.[6] Regardless, the legislation has forced businesses to closely evaluate exactly how and why they collect certain data points.

In the beginning of 2022 alone, four states—California, Kentucky, Maryland, and New York—all proposed standalone biometric laws that parroted BIPA, even down to the fulsome private right of action.[7]

California

The earth-shattering California Consumer Privacy Act of 2018 ("CCPA" or the "Act"), effective as of 2020, included biometric data in its definition of personal information.[8] In fact, the CCPA definition is more expansive than that contained in BIPA, including things that can be used to establish an individual's identity, such as vein patterns, keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data.[9] The CCPA generally treats biometric information in the same way that it treats other personal information. However, this was not enough for California legislators.

In November 2020, California passed the California Privacy Rights Act ("CPRA") that amended and expanded upon the CCPA. Pursuant to the CPRA, biometric data means a characteristic that "is used or is intended to be used" to establish a person's identity.[10] In addition, biometric information is now part of the "sensitive personal

©2026 Troutman Pepper Locke

information" category, which means that businesses are further limited in how they can use that data.[11]

In February 2022, a California state senator introduced SB 1189, or the California Biometric Information Privacy Act, which supplements the CCPA and CPRA.[12] Notably, it broadens the definition of biometric information from that included in the CCPA and CPRA. Now, biometric information would mean an individual's data "generated by automatic measurements of an individual's unique biological or behavioral characteristic, including a faceprint, fingerprint, voiceprint, retina or iris image, *or any other biological characteristic that can be used to authenticate the individual's identity*."[13] As a result, the proposed law could cover someone's physiological information (such as vein patterns), as well as behavioral characteristics (such as how someone types). This definition is likely to cover some of the same data as the CCPA and CPRA. But the inclusion of the catch-all definition is notable and may lead to some interesting claims by creative plaintiffs.

SB 1189, if passed, regulates a wide variety of conduct and would require a company to take proactive and comprehensive steps to ensure compliance. The regulated conduct includes, among other things, the collection, use, transfer, processing, capture, disclosure, storage, and transmission of the biometric data. Importantly, the company must obtain consent from the consumer before collecting the data and publish a policy establishing the retention schedule and guidelines for permanently destroying the biometric information.[14]

The proposed law includes a private right of action for consumers, which is likely to lead to an increase in litigation involving California consumers. While the statutory damages are less than in Illinois, between $100, and $1,000 per violation, per day,[15] the damages would quickly add up to potentially catastrophic amounts.

Kentucky

The proposed Kentucky legislation, HB 626, is essentially a copycat of BIPA and utilizes substantially the same definition of "biometric identifier."[16]

Like its Illinois statutory inspiration, this law would prohibit companies from utilizing biometric information for commercial purposes, unless the person is informed of the practice to obtain the data before it is actually captured and provides the requisite consent. Once in possession of the biometric data, a company cannot disclose it to a third party unless the person provides express consent or authorization. Additionally, companies implicated by this law would be required to provide privacy policies and guidelines for retaining and destroying biometric data. Businesses would also be required to employ reasonable security measures to safeguard the information. The proposed legislation includes a Gramm-Leach-Bliley Act exemption for covered entities.

Unlike BIPA, though, HB 626 does not provide a private right of action. Only the attorney general can bring enforcement actions for violations. The law would levy heavy fines against violators with civil penalties of up to $2,000 per violation that can be quintupled if the affected individuals are over the age of 60.[17]

Maryland

HB 0259, or the Biometric Data Privacy Act ("BDPA") is also based on BIPA and would provide comparable protections to consumers. The bill defines biometric data similarly to other statutes, particularly as data generated by automatic measurements of the biological characteristics of an individual. This includes fingerprints, voiceprints,

an eye retina, an eye iris, or any other unique biological patterns or characteristics that is used to identify a specific individual.

A private entity in possession of biometric data must develop a publicly available written policy that establishes a retention schedule and guidelines for the permanent destruction of the data.[18] Any private entity in possession of biometric information must store, transmit, and protect it from disclosure using reasonable standard of care within the industry, and in a way that is as protective, or more protective, than the way it treats other confidential and sensitive information. Companies are also required to ensure any of their processors (entities that process, store, or use biometric data on behalf of the company) comply with the proposed law.

The proposed Maryland legislation does provide for a private right of action, enabling individuals to seek damages from the private entity for violations of the BDPA.[19] A consumer is also permitted to request what biometric information is collected by a business, including the type of biometric data, and the purposes for which the private entity used the biometric data.[20]

New York

New York State has proposed its own Biometric Privacy Act (the "BPA") with Assembly Bill 27 following the amendment of New York City's administrative code to implement a similar law last year.[21] The BPA is also modeled on BIPA and defines biometric identifier in the same way – namely a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[22]

Just like its Illinois counterpart, BPA would require companies to develop a policy that is publically available regarding the retention schedule and guidelines for destruction of biometric data. Moreover, a private entity is prohibited from collecting, capturing, purchasing, receiving, or obtaining a person's biometric identifier or information unless it informs the subject in writing of the data being collected, explains the purpose and length of term for the collection and storage, and receives a written release by the individual.

Like BIPA, New Yorkers would have a private right of action that could lead to significant statutory liability in the event of a violation of BPA. The proposed legislation includes statutory damages of $1,000 per negligent violation and $5,000 per intentional or reckless violation. If the legislation passes, there may be a tidal wave of class actions filed against companies doing business in New York.

Takeaways

Legislators and regulators are focused on the collection, use, storage, and dissemination of biometric information and this interest is not likely to dissipate in the near future. Additionally, the increase in the number of states considering creating a private right of action for consumers means that companies are also likely to face a flood of litigation, similar to the experience of those entities subject to BIPA. Developing a compliance program is critical, as failure to do so can be very costly.

The majority of the pending legislation is substantially similar to BIPA in terms and scope. Consequently, entities may be able to employ similar policies and procedures to their use of biometric information, regardless of jurisdiction. Also, businesses must not only ensure that they have provided proper notice to the relevant

individuals when collecting data, but that they have a way to track the consumer's consent to the use of such information. Additionally, if a consumer denies permission to collect, use, or store this information, the company should have a process in place to make sure this decision is honored. One way to minimize any difficulties associated with compliance of these laws is to make sure that the company is only collecting the data that is essential to their operations and deciding carefully how to use and store data and over what period of time.

As states decide to jump into the biometric waters, it is imperative to stay on top of changes to confirm that a company's policies and procedures do not violate any nuance or change in the new laws. Regular conversations with stakeholders and outside counsel to craft and revise the relevant notices, policies, and procedures is an important and useful way to help reduce a company's exposure to possible violations of the existing and impending biometric information privacy laws.

***

[1] 740 ILCS 14/1 (2008).

[2] See Locke Lord companion articles about Illinois case law developments about the application of BIPA and growing case law concerning disputes over insurance coverage for BIPA claims.

[3] *See* Ark. Code § 4-110-104 (amended in 2019 to include biometric data in the definition of "personal information"); Cal. Civ. Code § 1798.100 (including biometric data in the California Consumer Privacy Act).

[4] *See* Tex. Bus. & Com. Code § 503.001 (the Capture or Use of Biometric Identifier Act or "CUBI"), Wash. Rev. Code § 19.375.020.

[5] Cal. Civ. Code § 1798.100.

[6] Ark. Code § 4-110-104; Tex. Bus. & Com. Code § 503.001; Wash. Rev. Code § 19.375.020.

[7] While Maine, Massachusetts, and Missouri are sometimes identified as states that have introduced biometric ?legislation based on BIPA, these bills are not addressed in this article. Both the Maine and Missouri proposals have ?stalled and the Massachusetts bill is not limited to biometric information?.

[8] Cal. Civ. Code § 1798.140.

[9] *Id*.

[10] Cal. Civ. Code § 1798.140(c).

[11] Cal. Civ. Code § 1798.100(a).

[12] S.B. 1189, 2021-2002 Reg. Sess., §§ 1798.301-304 (Cal. 2022).

[13] SB 1189, sec. 1798.300(a)(1) (italicize added).

[14] Cal. Civ. Code §1798.301(a) (Cal. 2022).

[15] Cal. Civ. Code §1798.304 (Cal. 2022).

[16] Ky. 22 RS BR 2162.

[17] *Id*. at § 2.

[18] The policy does not have to be made public if it only applies to the company's employees and is used solely for internal company operations.

[19] HB 259 at § 14-4406.

[20] *Id*. at § 14-4405.

[21] NYC Admin. Code §§ 22-1201-1205 (2021).

[22] Assembly Bill 27, § 676-a.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber