New 2023 Legislative Proposals Could Reshape the Biometric Privacy Landscape

Article By:
Kyle R. Fath
Kristin L. Bryan
David J. Oberly

New Year, New Bills

As Privacy World reported, 2022 saw a plethora of class action litigation stemming from alleged non-compliance with the well-known Illinois Biometric Information Privacy Act (“BIPA”). At the same time, due to concerns about companies using biometrics in a safe and responsible manner, lawmakers from coast to coast also attempted (albeit unsuccessfully) to put in place their own regulation to govern biometrics during the 2022 legislative cycle. Predictably, much of the same has taken place at the outset of 2023, with a total of nine states having already introduced biometrics-focused legislative proposals in January alone.

Below, we break down the bills that have been introduced in 2023 and what they would mean for companies if enacted.

Background: What Does BIPA Do?

As a refresher: under BIPA, which was enacted in 2008 and was the first state biometric privacy bill in the U.S., companies that collect or possess biometric data must adhere to a range of core compliance obligations:

- Under Section 15(a), companies must maintain a publicly-available privacy policy which includes, at a minimum, the company’s schedule and guidelines for permanently destroying biometric data.
- Under Section 15(b), companies must provide notice and obtain consent before collecting biometric data.
- Under Section 15(c), companies must refrain from leasing, trading, selling, or otherwise profiting from biometric data.
- Under Section 15(d), companies must refrain from disclosing biometric data unless consent is first obtained for the disclosure or, alternatively, if one of three exemptions applies to the
disclosure.
- Finally, under Section 15(e) companies must maintain security measures designed to safeguard biometric data.

Individuals “aggrieved” by a violation of BIPA may pursue class action litigation for non-compliance and are entitled to recover $1,000 per each negligent violation of the law and $5,000 per intentional or reckless violation, along with attorney’s fees.

**Breakdown of 2023 Biometric Privacy Legislative Proposals**

Notably, the bills introduced at the outset of 2023 are all closely patterned after BIPA—imposing similar compliance obligations and providing for the ability for individuals to pursue class action litigation for mere technical non-compliance. With that said, a number of the 2023 biometrics bills also contain unique compliance requirements that are not found in any active state or municipal biometrics statutes currently in effect. The end result of these pieces of legislation is that companies may see expanded exposure similar to that of BIPA, as well the need to make significant changes to their existing biometric privacy compliance programs.

**Arizona “Act Relating to Biometric Information”**

On January 30, Arizona lawmakers introduced the “Act Relating to Biometric Information” (SB 1238). SB 1238 is a carbon copy of BIPA—imposing identical compliance obligations, as well utilizing a private right of action as the bill’s exclusive enforcement mechanism that allows anyone “aggrieved” by a violation of the law to pursue class action litigation and the recovery of statutory damages of $1,000 for each negligent violation of the law and $5,000 for each intentional or reckless violation.

**Hawaii Biometric Information Privacy Act**

On January 20, Hawaii lawmakers introduced the Biometric Information Privacy Act (SB 1085). SB 1085 parallels BIPA’s compliance obligations almost completely, with one major exception. Specifically, the Hawaii bill provides a single, fairly narrow exemption from its data retention and destruction obligations, allowing companies to retain biometric data for a longer period of time than is prescribed by law where the retention of such data is required for legal compliance purposes. Also like BIPA, the Hawaii bill utilizes a private right of action as its exclusive enforcement mechanism, allowing for the recovery of $1,000 to $5,000 per violation of the law.

If enacted, the Hawaii BIPA would take effect immediately upon its approval—which could create significant compliance challenges for companies that utilize biometric data in their commercial operations, especially if they do not have any type of biometrics compliance program in place at this time.

**Maryland Biometric Data Privacy Act**

On January 11, the Maryland House of Representatives introduced the Maryland Biometric Data Privacy Act (“BDPA”) (HB 33). A week later, the Maryland Senate introduced an identical bill (SB 169). Of note, in 2022 the Maryland House passed an identical biometrics bill (HB 259), but this legislation ultimately failed to garner enough support by the state’s Senate to become law.

Importantly, the BDPA not only incorporates many of BIPA’s core compliance obligations—such as
informed consent—but also includes a number of additional provisions that have traditionally been seen only in connection with broader consumer privacy statutes. As just one example, the BDPA provides data subjects with the “right to know,” which would compel companies to disclose a range of pieces of information regarding their collection and use of biometric data upon request. In addition, the BDPA’s data retention and destruction requirements mandate that covered businesses destroy biometric data within 30 days after a business receives a data subject request for the deletion of their biometric data—in essence, creating a consumer “right to delete” that must be adhered to by companies that fall under the scope of the legislation.

The other main distinction between the Maryland bill and Illinois’s BIPA pertains to their respective enforcement provisions. Unlike BIPA, which provides a private right of action as its exclusive enforcement mechanism, the Maryland bill not only includes a private right of action, but also affords the state’s attorney general with the authority to impose civil penalties of up to $10,000 per violation.

If enacted, the BDPA would go into effect on October 1, 2022—providing only minimal time for companies to build out or otherwise modify their compliance programs to achieve compliance with the BDPA.

Massachusetts Biometric Information Privacy Act

On January 20, Massachusetts lawmakers in both the House and Senate filed similar biometric privacy bills—referred to as the Massachusetts Biometric Information Privacy Act (HD 3053 and SD 2218). These two bills are similar to BIPA, but both depart from the Illinois law in several key respects.

Specifically, compared to BIPA, HD 3053:

- Provides more detailed, granular privacy policy disclosure requirements, as well as a requirement that covered businesses provide notice of any change in its policy to data subjects at least 20 days before any privacy policy change goes into effect;
- Includes a unique prohibition on the use of biometric data for “monetization” purposes; and
- In addition to providing a private right of action allowing for class litigation, the bill authorizes the state attorney general to pursue civil penalties for violations of the Massachusetts law.

Similarly, compared to BIPA, SD 2218:

- Introduces a unique compliance obligation that bars “commercial establishments”—defined as a “place of entertainment, retail store, or food and drink establishment”—from using any biometric data for identification (surveillance) purposes;
- Allows the state AG to impose civil penalties for violations of the law; and
- Provides higher damages awards in class action litigation; specifically, “no less” than $5,000 per violation (regardless of whether the violation was negligent or intentional/reckless), as well an additional damages award multiplier ranging from two to three times the original statutory damages award if the court finds that the violation was done willfully or knowingly.

Minnesota “Act Relating to Private Data and Establishing Standards for Biometric Privacy”

On January 30, Minnesota lawmakers introduced the Minnesota Biometric Privacy Act (SF 954). SF
954 is also similar to BIPA—containing identical compliance requirements and available remedies for non-compliance with the law.

**Mississippi Biometric Identifiers Privacy Act**

On January 12, Mississippi lawmakers introduced the Biometric Identifiers Privacy Act (HB 467). The Mississippi BIPA was very similar to the bills currently pending in the Maryland House and Senate (HB 33 and SB 169), in that the Mississippi legislation contained a number of consumer rights ordinarily confined to broader consumer privacy statutes. With that said, the Mississippi BIPA died in committee on January 31, eliminating the prospect of new biometrics regulation in the Magnolia State—at least for 2023.

**New York Biometric Privacy Act**

On January 17, 2023, New York lawmakers introduced the New York Biometric Privacy Act (AB 1362). The Empire State is no stranger to proposed biometrics legislation, having introduced identical bills during the two previous legislative cycles. The New York BPA also resembles Illinois’s BIPA—providing identical compliance obligations and the recovery of statutory damages ranging from $1,000 to $5,000 per violation in class action litigation. If enacted, the BPA would take effect 90 days after having become law.

**New York “Act Prohibiting Use of Facial Recognition System by Landlords on Residential Premises”**

In addition, on January 4 New York lawmakers also introduced a unique piece of legislation that prohibits the use of facial recognition technology by landlords on any residential premises in the state (AB 322). As many know, New York City recently enacted its Tenant Data Privacy Act (“TDPA”), which imposes a range of requirements and restrictions on the use of all types of biometrics by owners and landlords in apartment complexes and similar types of residential housing. With AB 322, New York has gone a step further by attempting to impose a blanket ban over facial biometrics use by Empire State landlords and property owners.

AB 322 defines facial recognition for purposes of the prohibition as both: (1) the automated or semi-automated process by which a person is identified or attempted to be identified based on the characteristics of their face, including identification of known or unknown individuals or groups; and (2) the automated or semi-automated process by which a person is identified or attempted to be identified based on the characteristics of their face, including identification of known or unknown individuals or groups. The bill defines “face recognition system” as “any computer software or application that performs facial recognition.”

Under AB 322, landlords are prohibited from obtaining, retaining, accessing, or using—on any residential premises: (1) any facial recognition system; or (2) any information obtained from, or by use of, a facial recognition system. AB 322 provides for both AG enforcement of civil penalties for non-compliance with the law, as well as a private right of action allowing data subjects to pursue $1,000 in statutory damages for each violation of the legislation through class action litigation.

**New York “Act Prohibiting Private Entities From Using Biometric Data for Advertising”**
Lastly, on January 20 New York lawmakers introduced a second unique pieces of legislation, this time focused on targeting the use of facial recognition for advertising and marketing purposes (AB S2390). This bill seeks to ban private companies from using biometric data for any advertising, detailing, marketing, promotion, or other related activities that are intended to influence sales, as well as any evaluation of the effectiveness of marketing practices. Absent from AB S2390 is any language providing for an enforcement mechanism for violations of the law. If enacted, this bill would take effect 30 days after it becomes law.

**Tennessee Consumer Biometric Data Protection Act**

On January 23, Tennessee lawmakers introduced the Tennessee Consumer Biometric Data Protection Act (SB 339). SB 339 is nearly identical to BIPA in terms of its compliance obligations and enforcement mechanism.

SB 339 diverges from BIPA’s statutory text by including detailed language focused on ascertaining the number of violations committed by a private entity. This particular language was likely included in the bill to avoid the uncertainty that has caused significant complexities and challenges for defendants in BIPA class action litigation pertaining to this issue, known as “claim accrual.” The Illinois Supreme Court is set to provide a definitive resolution on the issue of claim accrual in BIPA litigation when it renders its opinion in *Cothron v. White Castle Sys.*, No. 128004, currently pending before the Court at this time.

For additional information on the Cothron Illinois Supreme Court appeal, see our extensive Privacy World coverage [here](#), [here](#), [here](#), and [here](#).

If enacted, the Tennessee biometrics law would take effect on January 1, 2024.

**Vermont “Act Relating to Protection of Personal Information”**

On January 26, Vermont legislators introduced “An Act Relating to Protection of Personal Information” (H 121), which departs significantly from BIPA, including in regards to:

- Inclusion of detailed content criteria for providing individualized notice prior to the collection of biometric data;
- More flexibility in obtaining consent from data subjects, including through verbal assent or in any other way that is reasonably calculated to collect informed, confirmable consent; and
- An obligation to implement a mechanism to prevent the subsequent use of biometric data before any such data is collected or retained.

Moreover, unlike BIPA, H 121 offers both class action litigation and AG enforcement of civil penalties as enforcement methods for non-compliance with the Vermont biometrics law. If enacted, the Vermont legislation will take effect on July 1, 2023.

**Mitigating Biometric Privacy Risk Going Forward**

**Monitor Closely for Additional Legislative Developments**

As we noted earlier this year, as businesses across all industries increase their reliance on biometric data to improve the efficiency of their operations and satisfy consumers’ growing interest in this next-
generation technology, lawmakers are also greatly increasing their efforts to enact tighter regulations over the collection and use of biometric data. As this area of regulation continues to develop, be sure to stick with Privacy World: we’ve got you covered.

In addition, readers are also strongly encouraged to join SPB’s Kyle Fath and Kristin Bryan for a timely webinar on the evolving landscape of laws around biometric data. The program will offer an engaging discussion, including the advisory and litigation perspectives relating to privacy in the specific context of biometrics. Importantly, during the webinar Kyle and Kristin will provide a deep dive into many of the biometric privacy bills discussed in this post, as well as strategies for how companies can get ahead of the compliance curve by implementing proactive modifications to their biometrics compliance programs that take into consideration the common compliance components and themes of the biometric privacy legislation introduced to date in 2023.

For additional information and to register for the webinar, click here: The Expanding Landscape of Biometric Data Law: Where We Are and What’s to Come

© Copyright 2023 Squire Patton Boggs (US) LLP

National Law Review, Volumess XIII, Number 49

Source URL: https://www.natlawreview.com/article/new-2023-legislative-proposals-could-reshape-biometric-privacy-landscape