As States Attempt to Toughen Biometric Data Restrictions, Companies that Collect and Store Biometric Data Face Risk

03.15.2023

ATTORNEYS

Maureen E. Fulton

PRACTICE AREAS

Data Privacy and Security

Key Takeaways:

- Businesses that collect or possess biometric data—such as fingerprints, hand scans, and retina scans—should carefully assess their legal obligations in light of current and potential biometric privacy laws.
- Numerous state legislatures have introduced biometric data privacy laws that could change the compliance landscape, with nine proposals currently active as of March 15, 2023. This legislative push, coupled with two recent rulings from the Illinois Supreme Court involving the Illinois Biometric Information Privacy Act ("BIPA") that broadly construe BIPA's scope, should raise red flags for businesses that collect or possess biometric data.

In this article, we discuss the new biometric data privacy proposals, existing state biometric data privacy laws, and the recent developments in Illinois under BIPA. Additionally, we explain why businesses should take note of these developments, and propose action items for businesses that collect or possess biometric data.

Existing State Biometric Data Privacy Laws

Illinois, Texas, and Washington each have a biometric-specific privacy law. Illinois, which enacted BIPA in 2008, was the first state to enact a biometric data privacy law. Texas quickly

followed suit and enacted the Capture or Use of Biometric Identifier Act ("CUBI") in 2009. Washington enacted its biometric privacy law ("Washington Law") in 2017. While each law covers biometric data, they differ in some respects.

Each law's definition of biometric data—which can be generally defined as any biological data or characteristics that may be used to identify a person—is slightly different. For example, BIPA and CUBI both define biometric "identifiers" as retina or iris scans, fingerprints, voiceprints, and scans of hand or face geometry. However, BIPA contains an extensive list of exclusions, while CUBI contains none. Unlike BIPA and CUBI, the Washington Law does not limit its definition of biometric identifiers to a prescribed list.

Further, CUBI and the Washington Law do not require covered entities to maintain a publicly available, written biometric information policy. BIPA, on the other hand, requires covered entities to maintain such a policy, including their data retention schedule and guidelines for permanently deleting biometric identifiers and biometric information. Finally, while BIPA provides a private right of action for harmed individuals to sue, CUBI and the Washington Law are enforceable only by the states' Attorneys General.

All three laws require covered individuals and entities to use a reasonable standard of care to protect biometric data. What is "reasonable" will depend largely on the data security standards within a particular industry. BIPA and CUBI also require that biometric data be protected in a manner that is the same or more protective than the measures taken by the covered individual or entity to protect other types of sensitive or confidential information that they may possess. Further, all three laws require the destruction of biometric data after a certain period of time. Typically, the destruction requirement will be triggered when the initial purpose for collection of the data no longer exists. For example, if an employer collects biometric data of an employee for security purposes, that purpose will usually expire upon termination of the employment relationship.

Recent Developments in Illinois

Recently, the Illinois Supreme Court issued two rulings that could have a significant impact on businesses' potential liability exposure for violations of BIPA. On February 2, 2023, in the case of *Tims v. Black Horse Carriers, Inc.*,[1] the court held that the state's "catchall" five-year statute of limitations applies to causes of action arising under BIPA. The court rejected Black Horse's argument that the state's one-year statute of limitations, governing certain privacy claims involving publication like libel or slander, should also govern BIPA. The court also rejected the lower appellate court's approach, which applied the one-year limitations period to certain sections of BIPA, while applying the five-year limitations period to other sections of BIPA. The

court adopted the five-year limitations period for all sections of BIPA to ensure "certainty, predictability, and uniformity," and to better accomplish BIPA's policy objectives.

Two weeks later, in the case of *Cothron v. White Castle System, Inc.*,[2] the court held that a separate claim "accrues" for each alleged violation of BIPA. For example, a person could bring a claim related to each time his or her biometric data was allegedly collected or transmitted in violation of BIPA, rather than only being permitted to bring one claim based on the first alleged violation. This holding is important for two reasons. First, BIPA's damages provisions establish liquidated damages for each violation. This means that damage awards could quickly add up—instead of one claim based on one violation, there could be many claims for many violations brought by the same plaintiff. Second, each alleged violation restarts the "clock" on the five-year limitations period that was established in the *Tims* case. In other words, even if the initial violation occurred more than five years prior to commencement of a lawsuit, subsequent violations that occurred within the five-year limitations period would still be actionable.

New State Biometric Data Privacy Proposals

Businesses familiar with the requirements of BIPA will recognize that most of the current biometric privacy proposals are very similar. Namely, the proposed bills in Arizona (SB 1238), Minnesota (SF 954), Missouri (HB 1047), Tennessee (SB 0339 / HB 0932), and New York (A 1362). Each bill would create a private right of action, and each would provide similar remedies for violations of their provisions—chiefly, liquidated damages on a per-violation basis. The bills also similarly define key terms like "biometric identifier," and contain similar notice and consent requirements.

If enacted, courts in these states may look to case law interpreting BIPA as a starting point for interpreting their new biometric privacy laws. Such an action may help provide some consistency across states, which would alleviate some of the major compliance concerns that accompany the expansion of a state-level patchwork approach to privacy regulation. It is important to note, however, that state courts are not bound by other state court interpretations, and even minor textual differences in the laws may lead courts to different results.

Maryland's current proposal (SB 698) includes biometric data privacy as part of a larger consumer data privacy bill. One important distinction between the Maryland bill and the other proposals, as well as BIPA, is that most of its provisions are directed at the business-consumer context. The bill, in its current form, expressly excludes data collected in the course of an employer-employee relationship. Another Maryland bill (HB 33) represents a more BIPA-like approach, focusing on biometric data privacy. The bill would not exclude data collected in the course of an employer-employee relationship, and it would provide for a private right of action.

As States Attempt to Toughen Biometric Data Restrictions, Companies that Collect and Store Biometric Data Face Risk

Vermont (H 121) has biometric data provisions contained within a larger amendment to its current consumer protection law. Those provisions are similar to BIPA, with the only major difference being the possibility of stiff civil penalties, to be sought by the Vermont Attorney General, in addition to a private right of action with available monetary damages and equitable relief. Kentucky (HB 483) also allows a private right of action in addition to enforcement by its state Attorney General.

Massachusetts (H 63) currently represents the largest departure from BIPA of all the newly proposed bills. The bill has a more expansive definition of "biometric data" which includes "D.N. A. sequences, . . . gait, handwriting, keystroke dynamics, and mouse movements," in addition to "fingerprints, retina and iris patterns, [and] voiceprints." It would also require a more comprehensive "Biometric Privacy Policy" than what is required by BIPA, requiring such policies to include "use models," "all data management and security policies governing biometric information," and "all disclosure practices." All of that is in addition to the organization's retention schedule and guidelines for permanently deleting biometric information, also required under BIPA. The bill would create a private right of action, and it contains a similar remedy structure to BIPA.

Why This Matters For Your Business

Liability Exposure

The potential for a new patchwork of state biometric data privacy laws, as well as the Illinois Supreme Court's recent decisions construing BIPA, could substantially increase liability exposure for businesses that collect or possess biometric data. The potential for substantial damages awards was already illustrated in the case of *Rogers v. BNSF Railway Company*,[3] where a jury in federal district court found that BNSF recklessly or intentionally violated BIPA 45,600 times—one violation for each member of the plaintiff class. This triggered the $5,000-per-violation penalty contained in BIPA for intentional or reckless violations, amounting to a damages award of $228 million. The case is still in its post-trial stage, with an appeal by BNSF likely.

The combination of the potential for severe monetary damages illustrated by the *Rogers* case, combined with a five-year statute of limitations and a per-violation accrual of claims based on recent Illinois Supreme Court cases, means companies face harsh and long-lasting liability risk. Add in the potential for several new state biometric privacy laws being enacted this year, and it only increases that risk.

As States Attempt to Toughen Biometric Data Restrictions, Companies that Collect and Store Biometric Data Face Risk

Compliance Costs

As more states consider enacting new biometric data privacy laws, compliance becomes a growing concern for businesses that collect or possess biometric data of individuals who reside in multiple states. Although many of the proposed laws are similar in their current form, there is still plenty of time for amendments that could significantly alter their scope and enforcement.

For example, employers who have employees across multiple offices in multiple states would need to ensure that any biometric-based timekeeping or other security systems are compliant with all relevant state laws. The more laws there are, and the more differences there are between the laws, the higher the cost of ensuring compliance. These costs also include the necessity to many businesses of investing in more up-to-date and sophisticated cybersecurity programs to prevent data breaches.

Reputational Harm

Beyond liability exposure and compliance costs, businesses that violate biometric privacy laws and other privacy-related laws may risk reputational harm. Issues surrounding data privacy are front-of-mind for many companies. In addition to regulatory schemes like the California Consumer Privacy Act ("CCPA") and the European Union's General Data Protection Regulation ("GDPR"), consumer demands for increased privacy and better protection of their data from unauthorized disclosure has pushed businesses to update their data practices. Businesses that do not maintain compliance with data privacy laws may suffer reputational harm if they face regulatory inquiries for alleged violations of data privacy laws. This becomes even more true as more states enter the privacy regulation arena.

Action Items for Businesses

Reevaluate Compliance with Current Laws

Businesses should reevaluate their compliance with current biometric data privacy laws by:

- Determining whether the business collects or possesses biometric data (e.g., by using biometric timekeeping systems, access controls, etc.);
- Identifying whether any biometric data collected or possessed by the business is of Illinois, Texas, or Washington residents;
- Assessing the purpose for the collection of biometric data (i.e., commercial or non-commercial for purposes of Texas and Washington law); and

As States Attempt to Toughen Biometric Data Restrictions, Companies that Collect and Store Biometric Data Face Risk

- Ensuring their data retention and destruction policies are compliant with applicable state law, whether Illinois, Texas, Washington, or a combination.

Employers that utilize biometric timekeeping systems or other biometric-based systems that collect data from their employees in Illinois should seriously evaluate the necessity for such systems. If such systems are absolutely necessary, then ensuring compliance with BIPA, particularly its consent requirement, is crucial.

Assess Current Cybersecurity Infrastructure and Policies

While the importance of cybersecurity infrastructure and policies is not exclusive to biometric data privacy, it is an important aspect of compliance with existing laws, as well as any future laws. Covered entities may face liability if they fail to use reasonable care to protect biometric data.

Some cybersecurity best practices include:

- Implementing basic security measures for all employees (e.g., strong password requirements and two-factor authentication for account log-ins; Internet use protocols);
- Keeping computers and other company-owned, Internet-connected devices up-to-date;
- Ensuring networks are protected by firewalls, including work-from-home employees' home network, and ensure all networks are password-protected;
- Encrypting sensitive data (like biometric data) to help keep it protected in the event of a breach; and
- Implementing access controls to restrict employee access to sensitive data.

Actively Monitor Proposed Bills

Proposed biometric data privacy bills are currently active in Arizona (SB 1238), Kentucky (HB 483), Maryland (SB 698 and HB 33), Massachusetts (H 63), Minnesota (SF 954), Missouri (HB 1047), New York (A 1362), Tennessee (SB 0339 / HB 0932), and Vermont (H 121). Businesses with customers or employees in those states should monitor these bills as they progress through the legislative process. Doing so will enable businesses to get a head start on their compliance efforts—efforts that may prove daunting for businesses to which multiple new laws may apply.

Koley Jessen will continue to monitor developments related to biometric privacy laws and advise as updates become available. If you have questions, please contact one of the specialists in Koley Jessen's **Data Privacy and Security Practice Area**.

As States Attempt to Toughen Biometric Data Restrictions, Companies that Collect and Store Biometric Data Face Risk

Special thanks to Jacob Bishop, Koley Jessen Summer Associate, for his contributions to this article.

---

[1] 2023 IL 127801 (Feb. 2, 2023).

[2] 2023 IL 128004 (Feb. 17, 2023).

[3] No. 1:19-cv-03083 (N.D. Ill. Oct. 12, 2022).