

Guide to U.S. Biometric Privacy Laws

A Reference Guide to State Laws
on Biometric Information and
Related Legislative Trends



Published by:



Security Industry Association
8455 Colesville Road, Ste 1200
Silver Spring, MD 20910
info@securityindustry.org
securityindustry.org

The Security Industry Association (SIA) is the leading trade association for global security solution providers, with over 1,400 innovative member companies representing thousands of security leaders and experts who shape the future of the security industry.

©2023, Security Industry Association.
All rights reserved.

Co-Authored by:



Sean F. Darke, Esq.
Phillip Short, Esq.
Dykema Gossett, PLLC
10 S. Wacker St., Suite 2300
Chicago, Illinois 60606
SDarke@dykema.com
dykema.com

Dykema is a full service law firm that serves clients ranging from start-ups to Fortune 100 companies across the country in over 65 practice areas based in 14 offices nationwide, with a track record of understanding clients' businesses, applying experience and solutions driven approach to providing legal services, and helping clients achieve their business goals.

ABOUT THE AUTHORS

Sean F. Darke, Esq.

Sean Darke is an employment and labor litigator who has defended multiple class actions involving the Illinois Biometric Information Privacy Act.

Phillip Short, Esq.

Phillip Short is an attorney in Dykema's Business Litigation and Privacy and Data Security groups. As a Certified Information Privacy Professional (CIPP/US), Short assists public and private companies reduce their data privacy and cybersecurity risks and exposures.

Clay Cossé, Esq.

Clay Cossé represents clients in complex litigation in the automotive, products liability, commercial, electrical and gas utility, transportation, and catastrophic loss spheres.

Dante Stella, Esq.

Dante Stella is a senior member of Dykema's data security and privacy group, and counsels clients in complex disputes involving voluminous or sensitive data, responses to data security incidents, and information governance.

Jake Parker

Jake Parker is senior director of government relations for SIA with over 20 years of experience in public policy and advocacy in Washington, D.C., and state capitals around the country and as a congressional staff member.

Colby Williams

Colby Williams is associate director of government relations for SIA, bringing to the organization over seven years of experience in state government and public policy positions.

DISCLAIMER - THIS GUIDE IS PROVIDED SOLELY FOR INFORMATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSIDERED OR CONSTRUED AS LEGAL ADVICE ON ANY INDIVIDUAL MATTER OR CIRCUMSTANCE. THE DISTRIBUTION OF THIS GUIDANCE OR ITS CONTENT IS NOT INTENDED TO CREATE, AND RECEIPT OF IT DOES NOT CONSTITUTE, AN ATTORNEY-CLIENT RELATIONSHIP OR LEGAL ADVICE. THE VIEWS AND OPINIONS EXPRESSED IN THIS GUIDANCE ARE THE AUTHORS' OPINIONS ONLY AND YOU SHOULD NOT ACT UPON THIS INFORMATION WITHOUT SEEKING LEGAL ADVICE FROM A LAWYER LICENSED IN YOUR JURISDICTION RELATING TO THE TOPICS CONTAINED IN THIS GUIDE. NEITHER DYKEMA, SIA NOR THE AUTHORS ARE RESPONSIBLE FOR ANY ERRORS OR OMISSIONS IN THE CONTENT OF THIS PRESENTATION OR FOR DAMAGES ARISING FROM THE USE OR RELIANCE UPON THIS PRESENTATION UNDER ANY CIRCUMSTANCES.



TABLE OF CONTENTS

Introduction.....	4
States With Biometric Privacy Laws	7
Illinois.....	7
Texas	12
Washington	13
States With Comprehensive Data Privacy Laws Addressing Biometrics.....	14
California	14
Colorado.....	16
Connecticut.....	17
Delaware.....	17
Indiana	18
Iowa.....	18
Montana.....	19
Oregon.....	20
Tennessee.....	20
Texas	21
Utah.....	22
Virginia.....	22
States With Health Care Data Privacy Laws Addressing Biometrics	24
Washington	24
Nevada	25
States With Data Breach Notification Laws Addressing Biometrics.....	27
Additional Unique Laws on Biometrics.....	27
New York.....	27
Appendix – Sample Consent for BIPA Compliance.....	29



INTRODUCTION

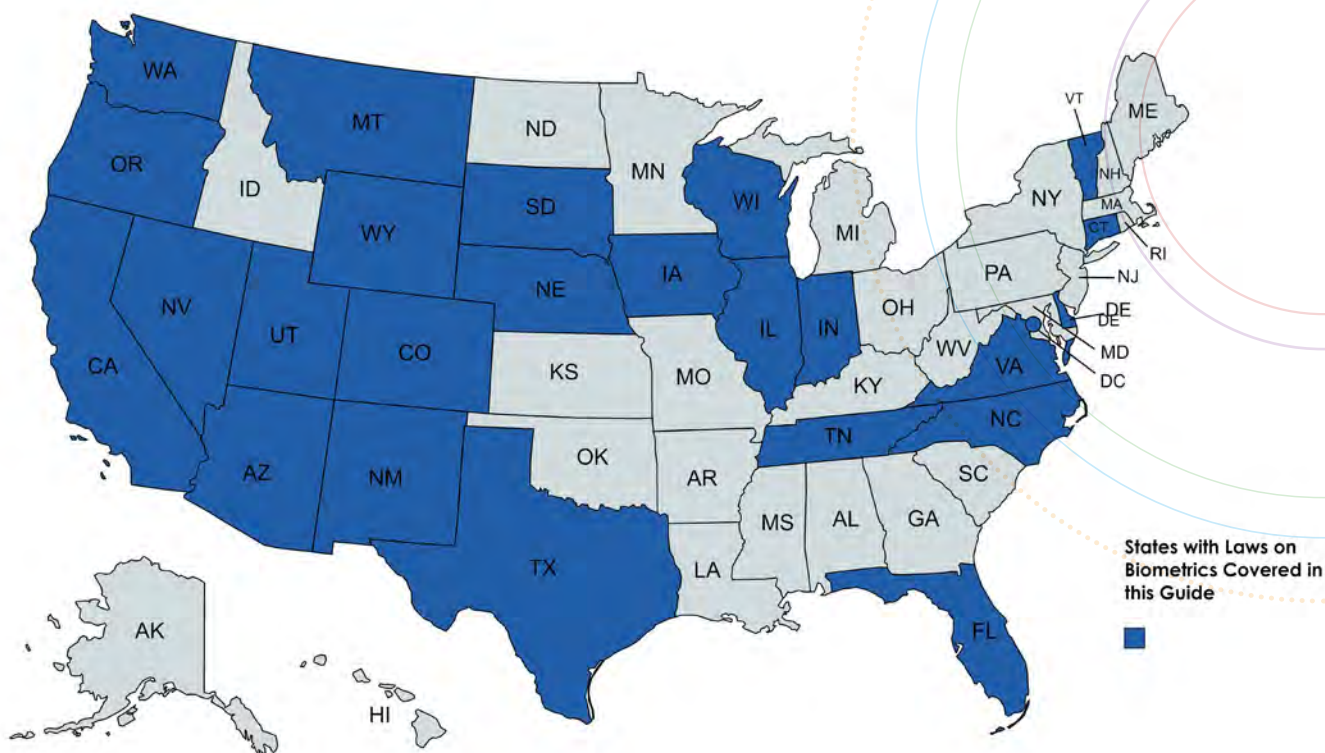
Welcome to the first edition of the Security Industry Association (SIA) Guide to Biometric Privacy Laws for SIA members.

As state-level data privacy laws continue to be enacted across the country, and clarified by state courts, this guide can serve as a starting point for any business user or industry supplier of biometric technologies attempting to navigate the legal landscape around biometrics throughout the United States, which can be complex. Businesses need to be proactive in their compliance quests. In particular, as we have seen in Illinois, a court's interpretation of the law can change businesses' compliance requirements quickly and impose instant litigation risks, which is why it's imperative that a business consult an attorney regarding maintaining compliance, as the laws and their interpretations evolve.

The Importance of Biometric Technologies

Biometric technologies create, compare and match data based on physiological (either morphological or biological) or behavioral measurements, to uniquely identify a person. Biometric data is the data that is created from those measurements.¹ The most common biometric technologies in use across government, commercial and consumer application today involve face, fingerprint, voice, iris or palm recognition. Recent advancements in computing power, artificial intelligence-driven software and industry innovation have made these technologies more affordable, accessible and ubiquitous in a wide variety of applications requiring more accurate and secure methods of identification. Biometric technologies have emerged as critical to the security field because they can enhance capabilities of solutions like video security, access control and identity management systems that help customers secure their facilities, employees and patrons against the threat of violence, theft or other harm.

¹For reference, under the European Union (EU) General Data Protection Regulation, "biometric data" is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data." See <https://gdpr-text.com/read/article-4/>.



SCOPE OF THIS GUIDE

This guide covers U.S. statewide laws that impose requirements specifically on use of biometric data and technologies, which apply generally to commercial and consumer use versus government. Some states and localities have also enacted laws specifically and solely addressing facial recognition technology, nearly all of which pertain to government use only. These laws will be covered in a separate *SIA Guide to State and Local Laws on Facial Recognition Technology*. The information in this guide is presented with suppliers and end users of safety and security-related applications of biometric technologies in mind, though SIA members may also develop and provide other types of applications as well.

Trends in Law

Several types of laws are covered in this report. Concerns around the security of biometric data led to the nation's first biometric data privacy law in Illinois in 2008, prior to widespread adoption at a time when the technology was little understood. The impact of flaws in this early law is still being felt and is even greater today, as detailed in this guide.

No state has since chosen to replicate the Illinois model, despite proposals in dozens of state legislatures, as a more comprehensive approach to data privacy is being adopted in the EU and the U.S. Of the modern measures, biometric data is considered one of many forms of personal data that are protected under a common framework.

While three states have enacted privacy laws specific to biometric data, they predate comprehensive state regulation that began in 2018. 13 U.S. states now have enacted comprehensive data privacy laws that include biometrics. Beyond the first, California, which was passed in 2018, the rest have adopted a common model (with a few differences),² which is based more closely on the framework and concepts from the EU's General Data Protection Regulation. Adoption of this model is swiftly increasing, with eight states enacting their own laws in 2023 alone, a trend that is likely to continue. The measures have received strong bipartisan support and have been successfully enacted in both "red" and "blue" states where state government is dominated by either Republicans or Democrats.

How to Get Involved

SIA members have the opportunity to make the most of their membership by getting more involved with our numerous committees, working groups, interest groups and advisory boards to help guide the association – and lead the industry – by defining policy; developing standards; planning education, training and professional development offerings; creating resources and member benefits; and organizing membership activities. For example, the SIA Identity and Biometric Technology Board is an advisory panel to the SIA Board of Directors which promotes the advancement and adoption of innovative biometric and digital identification solutions to secure critical assets, protect individual identity, safeguard propriety data and enhance consumer experience. Also, the SIA Data Privacy Advisory Board provides information and best practices to help SIA members handle sensitive data in a safe and secure manner to protect the personally identifiable information of their employees, partners and customers from potential breaches.

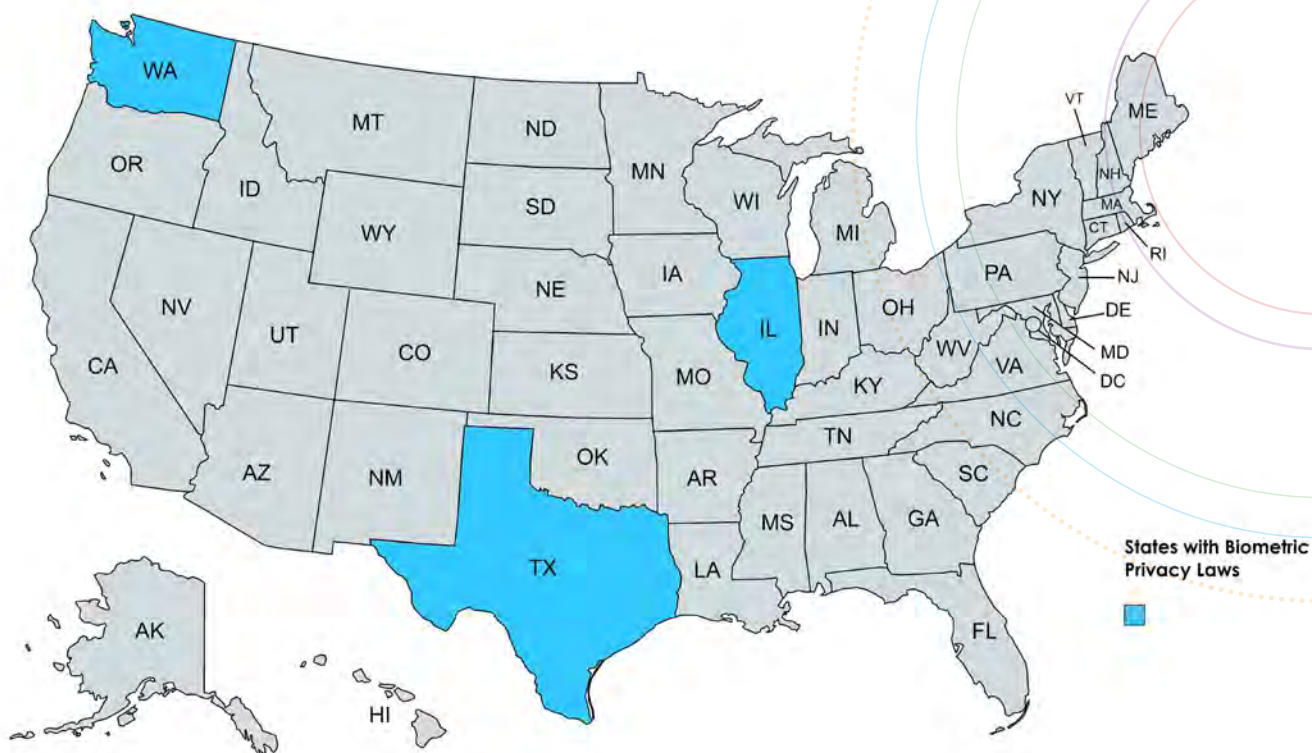
Check out SIA's Committee Guide³ to learn more about what each group does and how you can get involved. Additionally, you can volunteer⁴ to be an education and training leader, get involved in advocacy efforts, contribute to our publications and thought leadership and/or participate in SIA events.



²For a comparison, see <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>

³<https://www.securityindustry.org/about-sia/sia-committee-guide/>

⁴<https://www.securityindustry.org/about-sia/volunteer/>



STATES WITH BIOMETRIC PRIVACY LAWS


Only three states have broadly-applicable laws imposing requirements regarding biometric information.

STATE OF ILLINOIS

In 2008, the Illinois Biometric Information Privacy Act (BIPA)⁵ became the first state to enact biometric privacy law, and BIPA remains the only privacy law in the U.S. that provides a private right of action as an enforcement mechanism.

Illinois enacted BIPA to regulate the collection, use, safeguarding, handling, storage, retention and destruction of biometric identifiers. Although there was very little litigation in the years following enactment, since 2019 there has been a flood of class action litigation following key court interpretations of the statute. The first major decision was when the Illinois Supreme Court in *Rosenbach v. Six Flags Entertainment Corp.* held that a business only needs to violate the procedural steps laid out in BIPA to be liable for damages, versus violations resulting in harm to a consumer.

⁵ <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>



BIPA defines “biometric identifier” as “retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.” However, BIPA additionally uses the term “biometric information,” defined as “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.”

Who is subject to BIPA? Any private entity that is “in possession” of biometric identifiers or biometric information. A “private entity” is defined as any “individual, partnership, corporation, limited liability company, organization, or other groups, regardless of how it is set up.” It is important to remember that BIPA is not simply an employer/employee statute – it is much broader. BIPA applies broadly to any “private entity,” which does not include a state or local government agency.

A private entity subject to BIPA requirements needs to obtain a “written release,” which means “informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.” See in the attached **Appendix** a sample notice and release, which should be reviewed and discussed with an attorney for compliance prior to any use.

Another key requirement of BIPA is for each private entity to have a written policy on destroying any stored biometric identifiers or biometric information. This written policy must contain an retention schedule and guidelines that lay out the permanent destruction of the biometric identifiers and biometric information that are being stored by the private entity. BIPA requires the destruction either (1) when the initial use of collecting those identifiers or information has been satisfied or (2) within three years of the individual’s last interaction with the private entity, whichever occurs first.

If a private entity collects, captures, purchases, receives through trade or otherwise obtains a person’s or customer’s biometric identifier or biometric information, the private entity must do the following:

1. inform the individual in writing that a biometric identifier or biometric information is being collected or stored;
2. inform the individual in writing of the specific purpose and how long the biometric identifier or information is being collected, stored and used; and
3. obtain a written release.

Important Case Law

In addition to *Rosenbach v. Six Flags Entertainment Corp.*, recent key court decisions continue to shape an evolving interpretation of BIPA requirements and litigation. Some have provided helpful clarifications, but most have served to make BIPA class actions even more lucrative for the trial bar, at the expense of businesses.

In *Barnett v. Apple, Inc.* (2022) a plaintiff's complaint that Apple, Inc. ("Apple") violated BIPA was dismissed. The plaintiff's complaint involved using her own device to capture and collect her own information, which was stored on her device. The court held that the plaintiff could have deleted or stopped using the feature. Further, in this matter, the plaintiff did not allege that the biometric identifier(s) or information was transferred or stored on a separate server. In 2022 *Zellmer v. Meta Platforms* was dismissed in the U.S. District Court and, the case is currently on appeal to the Ninth Circuit. Involving a now discontinued Facebook feature called Tag Suggestions, the court dismissed the plaintiff's claim that BIPA's written consent requirement extends even to nonusers of a system or a service, with whom the provider has no relationship, and "scans" are only momentarily compared in order to determine whether an individual is an enrolled user, as an outcome the court argued was never intended under BIPA. This same ability is key for BIPA-compliant security applications of biometric technologies – for example, an access control system must distinguish between authorized users and those that are unauthorized. See SIA's amicus brief supporting the District Court decision for more information.⁶


POLICY PERSPECTIVE: BIPA Reform Gaining Traction

During the 2023 legislative session, Illinois state legislators, statewide officials, business leaders and industry representatives worked together to develop BIPA reform legislative proposals. While these efforts did not make it to enactment into state law, they gained significant bipartisan support, including proposed legislation authored by Senate President Pro Tempore Bill Cunningham (D-Chicago) adding a security exception (see below), which indicates potential for enactment of reform in the future.

Specifically, the Illinois business community has called for the following amendments to BIPA:

1. A "cure" process allowing technical violations discovered to be corrected within a set period of time without penalty
2. Clarifying that damage liability is per-person and per-section, versus "per-scan"
3. Providing an exception for biometric information collected and used for security purposes
4. Clarifying a the definition of a biometric "scan"
5. Specifically allowing for electronic consent
6. Allowing "evergreen" consent similar to the Health Insurance Portability and Accountability Act (HIPAA)
7. Specifying a one-year statute of limitations, versus five under current case law

⁶ <https://www.securityindustry.org/2023/10/05/sia-files-amicus-brief-in-key-bipa-case/>



On the other hand, in *McDonald v. Symphony Bronzeville Park*, the Illinois Supreme Court decided on Feb. 3, 2022, that the Illinois Worker's Compensation Act does not preempt BIPA. While more than 1,500 cases have been filed under BIPA resulting in over \$2 billion in settlements, only one has made it to a trial verdict where violations were actually proven in court. In that case, the U.S. District Court for the Northern District of Illinois awarded damages to the class for \$228 million in damages against BNSF Railway; however, the judge then granted a new trial for damages only that was set for Oct. 2, 2023. The parties have since agreed to settle, for which the monetary amount will be made public in late October/early November 2023.

On Feb. 2, 2023, the Illinois Supreme Court handed down a long-awaited decision on which statute of limitation applies, which further exposes businesses. In *Tims v. Black Horse Carriers, Inc.*, the Illinois Supreme Court held that the five-year statute of limitations applies to BIPA claims, versus one year. This means that an individual has five years after an alleged violation to bring an action under BIPA against a business. To make matters worse, in *Cothron v. White Castle Systems, Inc.* the Illinois Supreme Court held on Feb. 17, 2023, that "a separate claim accrues under BIPA each time a private entity scans or transmits an individual's biometric identifier or information," meaning in that particular case penalties could reach \$17 billion.

BIPA provides that any violation can result in liquidated damages of \$1,000 or actual damages, whichever is greater; if intentional or reckless violation results in liquidated damages of \$5,000 or actual damages, whichever is greater, reasonable attorney fees and costs, includes expert witness fees and other litigation expenses, other relief, including an injunction as the state of federal court may deem appropriate.

Major Settlement Examples

- Facebook (\$650 million, photo tagging feature); TikTok (\$92 million, facial filter technology); Google, Inc. (\$100 million, Google Photos app); McDonald's (\$50 million, collection of biometrics).
- *Bryant v. Compass Group USA, Inc.*, Case No. 1:19-cv-06622 (N.D. Ill.) – alleged that vending machines collected fingerprints for touchless payment without consent (\$6.8 million)
- *Williams, et al. v. Personalizationmall.com LLC*, Case No. 1:20-cv-00025 (N.D. Ill.) The employer used fingerprint scanner to clock employees in and out of work (\$4.5 million settlement)
- *Phillips v. BioLife Plasma, LLC*, Case No. 2020 CH 05758 (Cook County). Plaintiff alleged that defendant failed to store, transfer and maintain fingerprints collected from plasma donors in accordance with BIPA (\$5.99 million settlement)

At the most basic level, here are BIPA requirements that should be part of any company's compliance checklist:

- A publicly available written policy establishing a retention schedule governing how long biometric information will be retained and guidelines for the destruction
- An internal policy ensuring the required procedures, including the collection of a written release, will be followed in collecting biometrics and in any disclosure of biometric information outside the organization
- Establishing the steps required for securing any biometric information in possession

POLICY PERSPECTIVE: Replicating BIPA in Other States?

Despite frequent introduction of proposed legislation in other states that copy Illinois BIPA, these proposals have been continually rejected by state legislatures around the country. In fact, no other state has adopted this approach. In 2023, this trend continued, as such measures have failed in 12 states. Working with the business community and across many sectors, SIA has engaged directly with lawmakers in each of these states, providing testimony and other information urging alternative approaches.

SIA supports common-sense protections for biometric data and the responsible, ethical implementation of biometric technologies, but for years BIPA has affected consumers in ways that were never intended, enriching trial lawyers instead of protecting consumer interests and making many beneficial technologies unavailable due to litigation risk. BIPA lawsuits have mostly involved noncontroversial uses of biometrics. 88% of



the cases have been related to biometric timekeeping for hourly employees to clock in to work. Where cases alleged "consumer harm," 20% of such cases have

involved virtual try-on services, and 40% have involved security and identity verification services. Across the spectrum of cases, 50% of suits are against small businesses.⁷ These outcomes, harmful to businesses and consumers alike, would multiply if such policies are extended to other states.

BIPA or BIPA-Similar Measures Proposals in 2023

- Failed at the Committee Level: AZ, TX, MN, MO, MS, KY, MD, ME
- Failed after Passing One Chamber: NV
- 2-Year Measures Failed to Advance in 2023: NY, MA, VT

⁷ See - <https://progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf>



STATE OF TEXAS

In 2009, the Texas Capture or Use of Biometric Identifiers Act (CUBI)⁸ was enacted to regulate the collection of biometric identifiers for a “commercial purpose.” Notably this term is not defined within CUBI or elsewhere in Texas law in direct relation to it. CUBI applies to all private entities, with the exception of voiceprint data retained by a financial institution or an affiliate of a financial institution. CUBI requires a business to provide notice and acquire consent before collecting any biometric data for a commercial purpose. In addition, CUBI requires businesses to destroy any biometric identifiers within a “reasonable time” and provides only a one-year window for businesses to permanently destroy any captured biometric data after its purpose has been fulfilled.

The Texas attorney general is responsible for enforcement of CUBI. Until recently there had been no complaints filed under the statute since its enactment; however, in 2022 Attorney General Ken Paxton filed the first complaints alleging violations of CUBI and the Texas Deceptive Trade Practices Act (TDPA), by Meta Platforms⁹ and Google¹⁰ respectively. These are still pending and in the early stages of litigation.

Subsequently, the Texas Data Privacy and Security Act (TDPSA),¹¹ a far more comprehensive data privacy law that also addresses biometric data, was enacted in 2023. TDPSA provides for various disclosure requirements related to personal data collection and processing, grants consumers the rights over their data, mandates that opt-outs be provided for specific data processing activities and imposes obligations on controllers/processors.

Similarly to CUBI, TDPSA requires businesses to gain consent before processing or disclosing biometric data; however, TDPSA additionally includes a clear exemption for data controllers/processors carrying out security functions (see further information on TDPSA in the next section).

There are no provisions within TDPSA indicating how the new requirements relate to CUBI when it comes to biometrics. Given that TDPSA will not be in effect until July 1, 2024, there is no existing case law or guidance on how the act will be implemented in this regard. Both acts are distinct laws, each with its own scope, and it appears for now that both laws will coexist and apply to different aspects of data privacy.

It is advisable for businesses operating or having significant sales in Texas that collect/process biometric data and personal data to ensure compliance with both laws until new guidance is available regarding any potential for overlap or conflict between provisions of CUBI and TDPA.

⁸ <https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm>

⁹ <https://texasattorneygeneral.gov/sites/default/files/images/child-support/State%20of%20Texas%20v.%20Meta%20Platforms%20Inc..pdf>

¹⁰ [https://www.texasattorneygeneral.gov/sites/default/files/images/press/The%20State%20of%20Texas's%20Petition%20\(Google%20Biometrics\).pdf](https://www.texasattorneygeneral.gov/sites/default/files/images/press/The%20State%20of%20Texas's%20Petition%20(Google%20Biometrics).pdf)

¹¹ <https://capitol.texas.gov/BillLookup/Text.aspx?LegSess=88R&Bill=HB4>



STATE OF WASHINGTON

Washington's biometric data privacy law¹² was enacted in 2017 and prohibits enrolling a person's biometric identifier in a database for a commercial purpose without taking specific measures. These measures include providing notice to individuals, obtaining their consent, or offering a mechanism to prevent the subsequent use of a biometric identifier for commercial purposes.

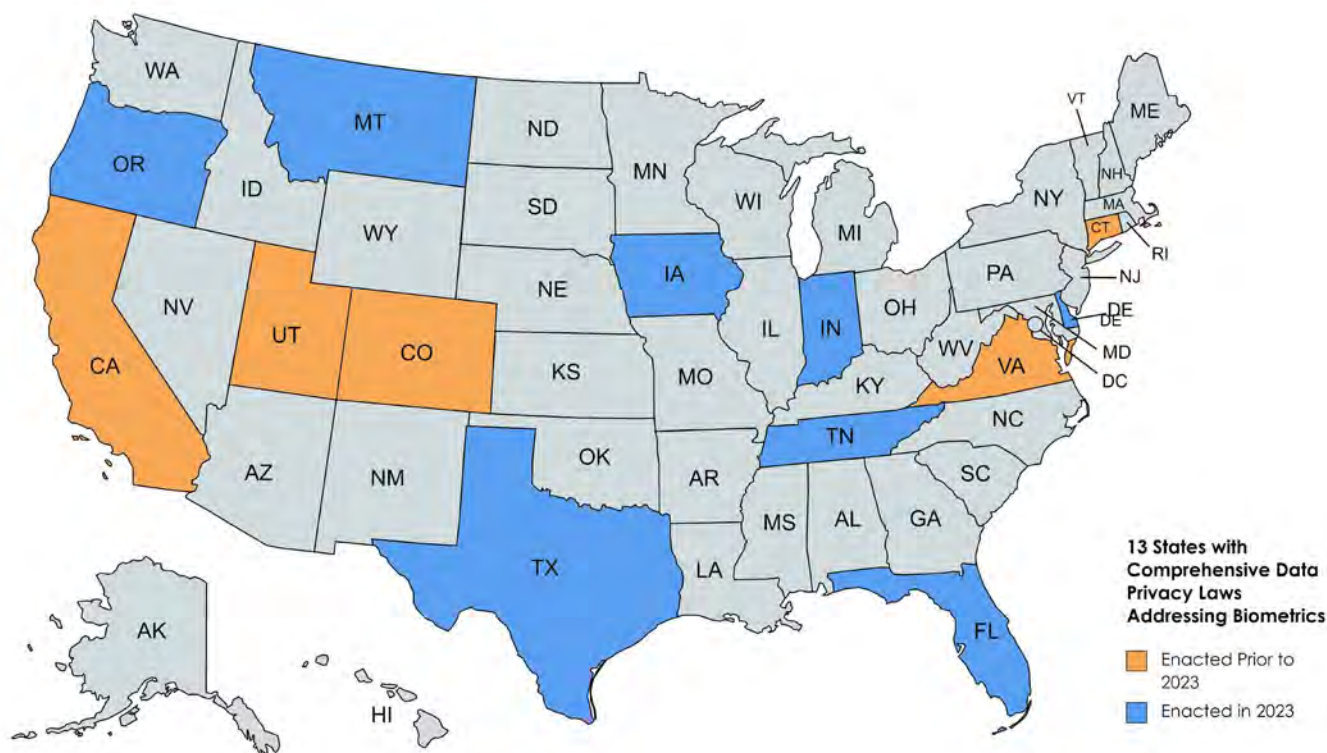
Under this law, "biometric identifier" is defined as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises or other unique biological patterns or characteristics that is used to identify a specific individual" but specifically excludes "a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used or stored for health care treatment, payment or operations under the federal health insurance portability and accountability act of 1996."

"Commercial purpose" specifically excludes a security or law enforcement purpose and is defined as "a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier."

The law provides an exemption for enrolling a biometric identifier and storing it in a biometric system in furtherance of a security purpose, which is further defined as "preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person."

This law falls under the purview of the Washington Consumer Protection Act and can be enforced by the Washington attorney general; however, no complaints alleging violations have been brought by the attorney general since the law's enactment.

¹² <https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true>



STATES WITH COMPREHENSIVE DATA PRIVACY LAWS ADDRESSING BIOMETRICS

Thirteen states now have enacted comprehensive data privacy laws that include biometrics. Outside California, the rest have adopted a similar model. These comprehensive data privacy laws generally create thresholds for applicability of the provisions of the law based on company size and revenue, allow for qualifying exceptions including security and use a narrowly tailored definition of biometrics and/or personal information. Each state also takes a varying approach to enforcement and civil penalties for violations, though all rely upon enforcement from the state attorney general as opposed to a private right of action. Measures enacted in 2023 have varying effective dates ranging from July 1, 2024 to January 1, 2026.



STATE OF CALIFORNIA

The California Consumer Privacy Act (CCPA)¹³ was enacted in 2018 as the nation's first state comprehensive data privacy law and was later expanded upon by the California Privacy Rights Act¹⁴ in 2020. California generally follows an approach providing consumers with a series of access and "opt-out" rights, contrasting with the GDPR and other state comprehensive

¹³ https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

¹⁴ https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

approaches requiring “opt-in” consent for collecting and processing personal data.

The California Privacy Protection Agency is charged with promulgating regulations to govern compliance with the CCPA. These regulations provide guidance to businesses on how to inform consumers of their rights established under the CCPA, how to handle consumer requests, how to verify the identity of consumers making requests and how to apply the law as it relates to various provisions and activities. Implementing regulations¹⁵ became effective on March 31, 2023.

The requirements apply to all entities doing business in the state that meet any of the following criteria: 1) have a gross annual revenue of over \$25 million; 2) buy, sell, or share the personal information of 100,000 or more California residents, households or devices; or 3) derive 50% or more of their annual revenue from selling California residents’ personal information.

Sensitive personal information under the law includes biometric information, which is defined as “an individual’s physiological, biological or behavioral characteristics, including information pertaining to an individual’s deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.”

The law generally requires organizations to provide consumers with the right to limit the use and disclosure of their sensitive personal information; however, Section 7027(m) of the regulations¹⁶ lists uses and disclosures of such information that do not trigger a requirement to post a notice of right to limit or provide a method for submitting a request to limit, provided that the use or disclosure is “reasonably necessary and proportionate” for those purposes. A number of these are relevant to security technology applications:

- 1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services
- 2) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity or confidentiality of stored or transmitted personal information
- 3) To resist malicious, deceptive, fraudulent or illegal actions directed at the business and to prosecute those responsible for those actions
- 4) To ensure the physical safety of natural persons

¹⁵ <https://cppa.ca.gov/regulations/>

¹⁶ https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf



Note, however, these exemptions only apply to the opt-out “right to limit.” Other obligations still apply, including requirements for collection, use, retention and/or sharing of personal information (Section 7002), which must a) be reasonable and proportionate to achieve its purpose b), be consistent with the reasonable expectations of the consumer or c) follow consumer consent. This necessitates determining needed compliance methods depending on the technology application.

STATE OF COLORADO

The Colorado Privacy Act¹⁷ (CPA) was enacted in 2021 and became effective July 1, 2023. It applies to business conducted in Colorado that satisfies one or both of the following thresholds: 1) the entity controls/processes the personal data of 100,000 consumers or more during a calendar year or 2) derives revenue or receives a discount on the price of services/goods from the sale of personal data and processes/controls the data of 25,000 consumers or more.

Under the Colorado law, “sensitive data” is defined to include biometric data, but the latter is not defined in the statute. However, within the implementation rules “biometric data” is defined as “Biometric Identifiers that are used or intended to be used, singly or in combination with each other or with other Personal Data, for identification purposes. Unless such data is used for identification purposes, “Biometric Data” does not include (a) a digital or physical photograph, (b) an audio or voice recording, or (c) any data generated from a digital or physical photograph or an audio or video recording.” In turn, “Biometric Identifiers” are defined as “data generated by the technological processing, measurement, or analysis of an individual’s biological, physical, or behavioral characteristics that can be processed for the purpose of uniquely identifying an individual, including but not limited to a fingerprint, a voiceprint, scans or records of eye retinas or irises, facial mapping, facial geometry, facial templates, or other unique biological, physical, or behavioral patterns or characteristics.”

The measure provides a security exception as follows: “The obligations imposed on controllers/processors under this act do not restrict their ability to...prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or malicious, deceptive, or illegal activity; preserve the integrity of security systems; or investigate, report, or prosecute those responsible for any such action.”

For more information, see the CPA implementation rules,¹⁸ which were finalized by the Colorado Attorney General’s Office in March 2023¹⁹ and have been in effect since July 1, 2023.

¹⁷ <https://leg.colorado.gov/bills/sb21-190>

¹⁸ <https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf>

¹⁹ <https://coag.gov/press-releases/3-15-23/>



STATE OF CONNECTICUT

The Connecticut Data Privacy Act²⁰ was enacted in 2022 and became effective on July 1, 2023. The act generally applies to “persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that during the preceding calendar year: (1) Controlled or processed the personal data of not less than one hundred thousand consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) controlled or processed the personal data of not less than twenty-five thousand consumers and derived more than twenty-five per cent of their gross revenue from the sale of personal data.” The Connecticut attorney general has provided additional helpful information about the law’s requirements.²¹

The definition of biometric data used is “data generated by automatic measurements of an individual’s biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual.” “Biometric data” does not include “(A) a digital or physical photograph, (B) an audio or video recording, or (C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.”

The measure provides a security exception as follows: “Nothing in this Act shall be construed to restrict a controller/processor’s ability to...prevent, detect, protect against or respond to security incidents, identify theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action.”



STATE OF DELAWARE

The Delaware Personal Data Privacy Act²² was enacted in 2023 and will become effective on Jan. 1, 2025. This act applies to entities/persons that conduct business in the state that “during the preceding calendar year did any of the following: (1) controlled/processes the personal data of not less than 35,000 consumers excluding personal data processed solely for the purpose of completing a payment transaction, (2) controlled/processes the personal data of not less than 10,000 consumers and derived more than 20 percent of their gross revenue from the sale of personal data.”

The definition of biometric data used is “data generated by automatic measurements of an individual’s unique biological characteristics, such as a fingerprint, a voiceprint, eye retinas,

²⁰ https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022

²¹ <https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act>

²² <https://legiscan.com/DE/text/HB154/id/2807502>

irises, or other unique biological patterns or characteristics that are used to identify a specific individual.” “Biometric data” as defined “does not include any of the following: a digital or physical photograph, an audio or video recording, any data generated from a photograph, audio or video recording, unless is generated to identify a specific individual.”

The measure provides a security exception as follows: “Nothing in this Act shall be construed to restrict a controller/processor’s ability to...prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any such activity.”



STATE OF INDIANA

The Indiana Consumer Data Protection Act²³ was enacted in 2023 and will become effective Jan. 1, 2026. This act applies to an entity that conducts business in Indiana that during a calendar year: 1) controls or processes the personal data of at least 100,000 consumers who are Indiana residents or 2) controls or processes the personal data of at least 25,000 consumers who are Indiana residents and derives more than 50% of gross revenue from the sale of personal data.

The definition of biometric data used is “data that: (1) is generated by automatic measurements of an individual’s biological characteristics, such as a fingerprint, a voiceprint, images of the retina or iris, or other unique biological patterns or characteristics; and (2) is used to identify a specific individual. (b) The term does not include: (1) a physical or digital photograph, or data generated from a physical or digital photograph; (2) a video or audio recording, or data generated from a video or audio recording; or (3) information collected, used, or stored for health care treatment, payment, or operations under HIPAA.”

The measure provides a security exception as follows: “This Act shall not be construed to restrict a controller/processor’s ability to...prevent, detect, protect against, or respond to security incidents, identify theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, investigate, report, or prosecute those responsible for any such action, and preserve the integrity or security of systems.”



STATE OF IOWA

The Iowa Consumer Data Protection Act²⁴ was enacted in 2023 and will be effective on July 1, 2025. This act applies to any business in the state of Iowa that during a calendar year does either of the following: 1) controls or processes personal data of at least 100,000 consumers or 2)

²³ <https://iga.in.gov/legislative/2023/bills/senate/5/details>

²⁴ <https://www.legis.iowa.gov/docs/publications/LGE/90/SF262.pdf>

controls or processes personal data of at least 25,000 consumers and derives over 50% of gross revenue from the sale of personal data.

The definition of “biometric data” used in this act is “data generated by automatic measurements of an individual’s biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. ‘Biometric data’ does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used or stored for health care treatment, payment, or operations under HIPAA.”

The act provides for the following full security exemption: “Nothing in this Act shall be construed to restrict a controller/processor’s ability to “prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, or to preserve the integrity or security of systems, or to investigate, report, or prosecute those responsible for any such action.”



STATE OF MONTANA

The Montana Consumer Data Privacy Act²⁵ was enacted in 2023 and will take effect on Oct. 1, 2024. This act applies to entities that conduct business in Montana that 1) control/process the personal data of not less than 50,000 consumers, excluding data for the sole purpose of completing a payment transaction or 2) control/process the personal data of not less than 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data.

The definition of “biometric data” used in this act is “data generated by automatic measurements of an individual’s biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual. The term does not include: a digital or physical photograph, an audio or video recording; or any data generated from a digital or physical photograph or an audio or video recording, unless that data is generated to identify a specific individual.”

The act provides a security exemption as follows: “Nothing in this Act shall be construed to restrict a controller/processor’s ability “to... prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, preserve the security or integrity of systems, or investigate, report, or prosecute those responsible for any of these actions.”

²⁵ [https://laws.leg.mt.gov/legprd/LAW0210W\\$BSIV.ActionQuery?P_BILL_NO1=384&P_BLTP_BILL_TYP_CD=SB&Z_ACTION=Find&P_SESS=20231](https://laws.leg.mt.gov/legprd/LAW0210W$BSIV.ActionQuery?P_BILL_NO1=384&P_BLTP_BILL_TYP_CD=SB&Z_ACTION=Find&P_SESS=20231)



STATE OF OREGON

The Oregon Consumer Privacy Act²⁶ was enacted in 2023, will be effective on July 1, 2024, and applies to any person that conducts business in Oregon, or that provides products or services to residents of the state, and that during a calendar year, controls or processes: 1) the personal data of 100,000 or more consumers, other than personal data controlled or processed solely for the purpose of completing a payment transaction, or 2) the personal data of 25,000 or more consumers, while deriving 25% or more of the person's annual gross revenue from selling personal data.

For the purposes of this act, "biometric data" means "personal data generated by automatic measurements of a consumer's biological characteristics, such as the consumer's fingerprint, voiceprint, retinal pattern, iris pattern, gait or other unique biological characteristics that allow or confirm the unique identification of the consumer. 'Biometric data' does not include: a photograph recorded digitally or otherwise; an audio or video recording; data from a photograph or from an audio or video recording, unless the data were generated for the purpose of identifying a specific consumer or were used to identify a particular consumer; or facial mapping or facial geometry, unless the facial mapping or facial geometry was generated for the purpose of identifying a specific consumer or was used to identify a specific consumer."

The act provides for the following security exemption: "this Act does not prohibit a controller or processor from 'Preventing, detecting, protecting against or responding to, and investigating, reporting or prosecuting persons responsible for, security incidents, identity theft, fraud, harassment or malicious, deceptive or illegal activity or preserving the integrity or security of systems.'"



STATE OF TENNESSEE

The Tennessee Information Protection Act,²⁷ enacted in 2023 with an effective date of July 1, 2025, applies to entities that conduct business in this state that: 1) during a calendar year, control or process personal information of at least 100,000 consumers; or 2) Control or process personal information of at least 25,000 consumers and derive more than 50% of gross revenue from the sale of personal information.

For the purposes of this act, "biometric data" means "data generated by automatic measurement of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retina or iris, or other unique biological patterns or characteristics that are used to identify a specific individual; and (B) Does not include a physical or digital photograph, video recording, or audio recording or

²⁶ <https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled>

²⁷ <https://www.capitol.tn.gov/Bills/113/Bill/SB0073.pdf>

data generated from a photograph or video or audio recording; or information collected, used, or stored for healthcare treatment, payment, or operations under HIPAA.”

The act includes the following security exemption: “This Act does not restrict a controller/processor’s ability to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activity, or illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for such action.”



STATE OF TEXAS

The Texas Data Privacy and Security Act (TDPSA)²⁸ was enacted in 2023 and will become effective July 1, 2024. Unlike other similar state laws with thresholds related to the volume of personal data held or related revenue, in Texas this broadly applies to any entity that:

- 1) conducts business in this state or produces a product or service consumed by residents of this state;
- 2) processes or engages in the sale of personal data; and
- 3) is not a small business as defined by the U.S. Small Business Administration

Note, however, that even if a business is considered a “small business” under this definition, restrictions on the sale of personal data still apply. Businesses cannot sell “sensitive” personal data, a category that includes someone’s race, religious beliefs, biometric data, sexuality and geolocation, before receiving consent from the consumer.

The TDPSA defines “biometric data” as “data generated by automatic measurements of an individual’s biological characteristics. The term includes a fingerprint, voiceprint, eye retina or iris, or other unique biological pattern or characteristic that is used to identify a specific individual. The term does not include a physical or digital photograph or data generated from a physical or digital photograph, a video or audio recording or data generated from a video or audio recording or information collected, used or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).”

The act includes the following security exemption: “Nothing in this Act shall be construed to restrict a controller/processor’s ability to ‘prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; or to preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security.’”

²⁸ <https://capitol.texas.gov/BillLookup/Text.aspx?LegSess=88R&Bill=HB4>



As noted in the previous section, it is not yet clear how TDPSA relates to requirements under CUBI when it comes to biometrics.

STATE OF UTAH

The Utah Consumer Privacy Act²⁹ was enacted in 2022 and will become effective on Dec. 31, 2023. The act applies to any controller/processor who: conducts business in the state; has annual revenue of \$25,000,000 or more; and satisfies one or more of the following thresholds: 1) during a calendar year, controls or processes personal data of 100,000 or more consumers; or 2) derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.

For the purpose of this act, "biometric data" means data generated by automatic measurements of an individual's unique biological characteristics. "Biometric data" includes data described in Subsection (6)(a) that are generated by automatic measurements of an individual's fingerprint, voiceprint, eye retinas, irises or any other unique biological pattern or characteristic that is used to identify a specific individual. 'Biometric data' does not include: a physical or digital photograph; a video or audio recording; data generated from an item described in Subsection (6)(c); information captured from a patient in a health care setting; or information collected, used, or stored for treatment, payment or health care.

The act creates two security-related exemptions; the first is cybersecurity-related. In the section regarding a consumer's right to opt out of the processing of their personal data, it appears as follows: "nothing in this section requires a person to cause a breach of security system as defined by 13-44-102." The second is a more full security exemption in the limitations section and is drafted as follows:

"The requirements in this Act do not restrict a controller/processor's ability to: 'detect, prevent, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity; or investigate, report, or prosecute a person responsible for an action described in Subsection (1)(h)(i); or preserve the integrity or security of systems; or investigate, report, or prosecute a person responsible for harming or threatening the integrity or security of systems, as applicable.'"

²⁹ <https://le.utah.gov/~2022/bills/static/SB0227.html>



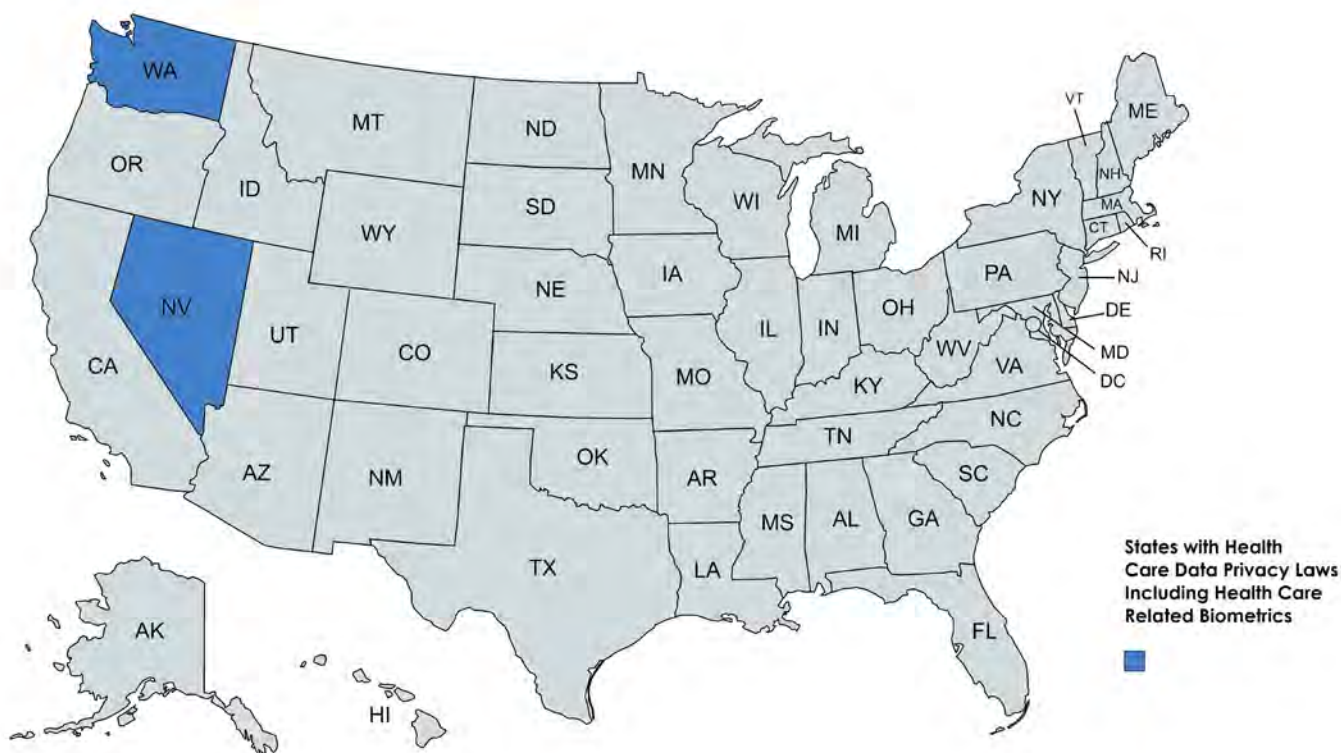
STATE OF VIRGINIA

The Virginia Consumer Data Protection Act³⁰ was enacted in 2021 with an effective date of Jan. 1, 2023, and applies to persons that conduct business in the commonwealth or produce products or services that are targeted to residents of the Commonwealth and that 1) during a calendar year, control or process personal data of at least 100,000 consumers or 2) control or process personal data of at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data.

For this act, “Biometric data” means “data generated by automatic measurements of an individual’s biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. ‘Biometric data’ does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA.”

This act provides a security exemption as follows: “Nothing in this Act shall be construed to restrict a controller/processor’s ability to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action.”

³⁰ <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53>



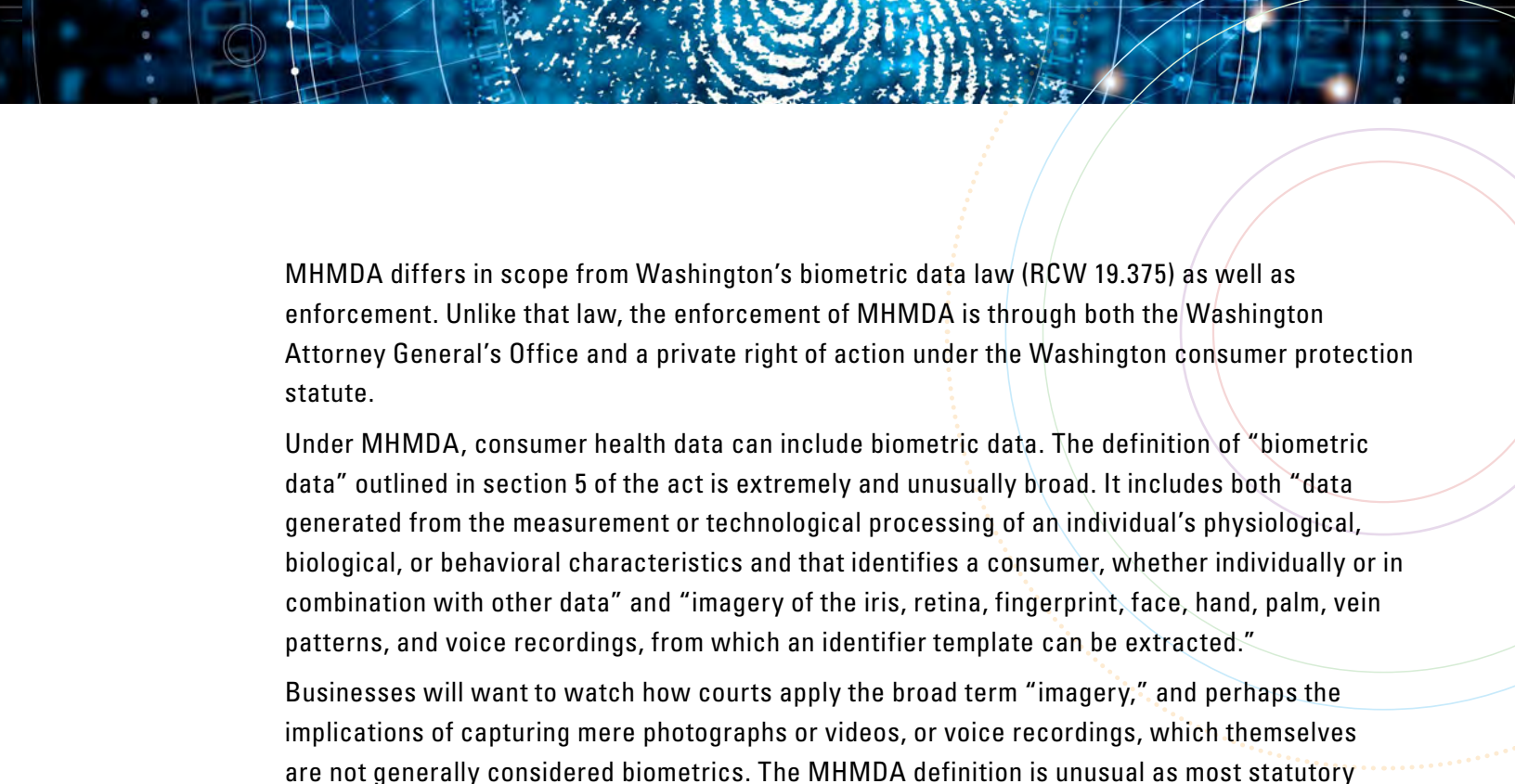
STATES WITH HEALTH CARE DATA PRIVACY LAWS ADDRESSING BIOMETRICS

Two states have recently enacted data privacy laws with applicability to biometrics, but specific only to consumer health data.

STATE OF WASHINGTON

In 2023 the state of Washington enacted the My Health My Data Act (“MHMDA”),³¹ most of which becomes effective March 31, 2024. The statute protects “consumer health data” collected by entities that fall outside of HIPAA, in the wake of the Dobbs Supreme Court decision and largely over concern for protecting reproductive rights. These protections are similar to common elements of broader data privacy laws, including consent for collection, notification for disclosure, prohibitions on the selling and sharing of data, etc. The law is applicable to all persons and businesses that collect, process, share or sell consumer health data in Washington (or provide services or products to Washington).

³¹ <https://app.leg.wa.gov/billsummary?BillNumber=1155&Year=2023>



MHMDA differs in scope from Washington's biometric data law (RCW 19.375) as well as enforcement. Unlike that law, the enforcement of MHMDA is through both the Washington Attorney General's Office and a private right of action under the Washington consumer protection statute.

Under MHMDA, consumer health data can include biometric data. The definition of "biometric data" outlined in section 5 of the act is extremely and unusually broad. It includes both "data generated from the measurement or technological processing of an individual's physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data" and "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted."

Businesses will want to watch how courts apply the broad term "imagery," and perhaps the implications of capturing mere photographs or videos, or voice recordings, which themselves are not generally considered biometrics. The MHMDA definition is unusual as most statutory definitions of biometrics specifically exclude physical or digital photographs and audio or video recordings.

The definition of "consumer health data" in MHMDA requires a personal health care context: "personal information that is linked or reasonably linkable to a consumer *and* that identifies the consumer's past, present, or future physical or mental health status" (emphasis added). However, the definition further states that "For the purposes of this definition, physical or mental health status includes, but is not limited to" 13 other elements, including among them simply, "biometric data." At the same time, the Washington Attorney General released a set of frequently asked questions (FAQs), which further emphasizes that "Information that does not identify a consumer's past, present, or future physical or mental health status does not fall within the Act's definition of consumer health data."³²

In any case, section 12 of the measure includes a security exception as follows: "(3) The obligations imposed on regulated entities, small businesses, and processors under this chapter does not restrict a regulated entity's, small business's, or processor's ability for collection, use, or disclosure of consumer health data to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any activity that is illegal under Washington state law or federal law; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action that is illegal under Washington state law or federal law. (4) If a regulated entity, small business, or processor processes consumer health data pursuant to subsection (3) of this section, such entity bears the

³² <https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy>

burden of demonstrating that such processing qualifies for the exemption and complies with the requirements of this section.” This makes applicability to most security products and services unlikely; however, if biometric data used is linked to health information or it involves identification in health care facilities or settings, this requires further analysis considering litigation risks presented by the private right of action.

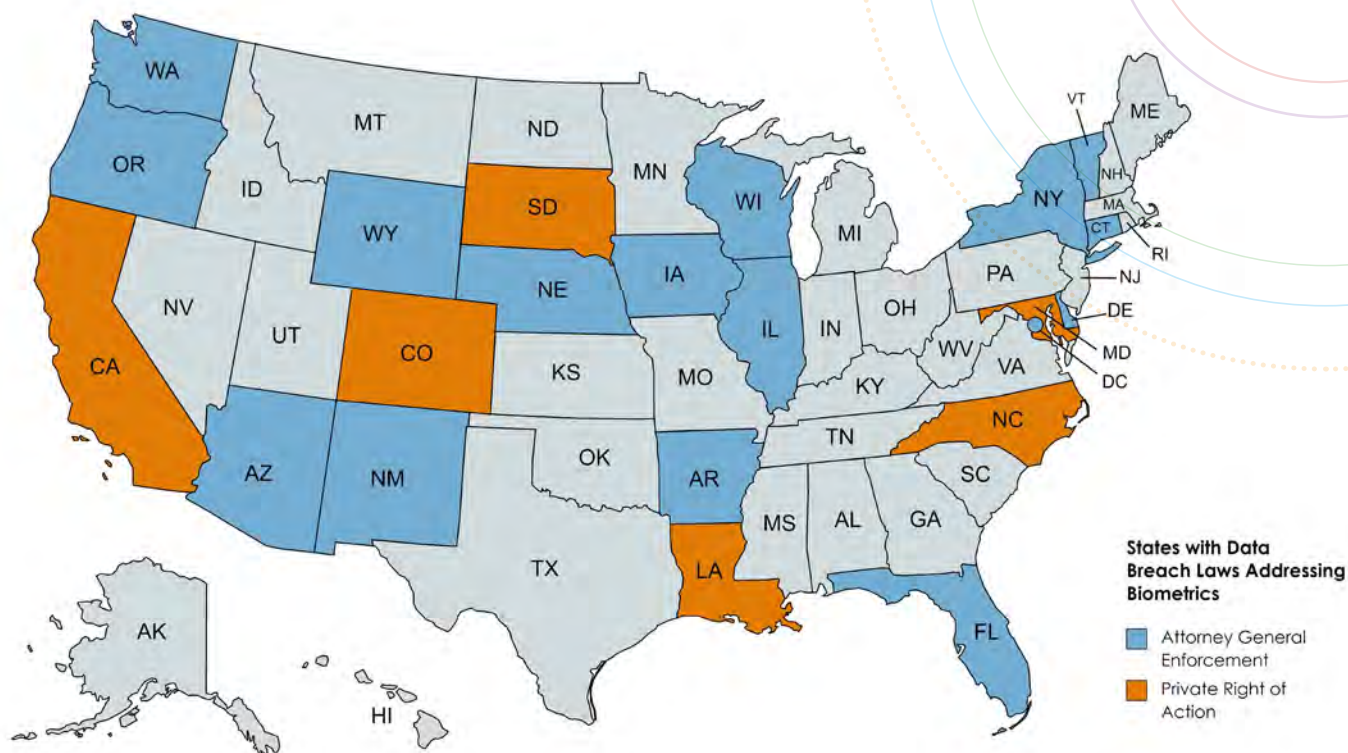


STATE OF NEVADA

In 2023, Nevada also passed a law specifically protecting consumer health data, SB 370,³³ which is based on and mostly similar to Washington’s MDHMDA and enacted for the same purpose. While its flawed definition of biometric data is nearly identical, and there is no security exception, as incorporated into the definition of consumer health data its applicability is narrower in two respects. First, for data to be considered consumer health data, it must be actually used by a regulated entity to “identify the past, present or future health status of the consumer.” Second, this includes biometric data only if it is related to “Information relating to: (1) Any health condition or status, disease or diagnosis; (2) Social, psychological, behavioral or medical interventions; (3) Surgeries or other health-related procedures; (4) The use or acquisition of medication; (5) Bodily functions, vital signs or symptoms; (6) Reproductive or sexual health care; and (7) Gender-affirming care.”

Another key difference with MHMDA is that the enforcement mechanism is solely through the state’s attorney general, versus a private right of action. Most provisions of Nevada’s law become effective March 31, 2024.

³³ https://www.leg.state.nv.us/Session/82nd2023/Bills/SB/SB370_EN.pdf



STATES WITH DATA BREACH NOTIFICATION LAWS ADDRESSING BIOMETRICS

All 50 states have laws requiring businesses, in certain circumstances, to notify individuals in the event of unauthorized access to their personal information, subject to applicability thresholds; however, in only some states is personal information defined to include biometric information. Of these, several provides a private right of action for individuals to recover actual damages from the failure to disclose in a timely manner to a person that there has been a breach.



ADDITIONAL UNIQUE LAWS ON BIOMETRICS

STATE OF NEW YORK

Effective since 2021, the City of New York's Biometric Identifier Information Law³⁴ imposes requirements on private entities, and the city is uniquely the only U.S. jurisdiction implementing a broad biometric data law at the municipal level.

First, the law prohibits the sale, lease, trade or other transactions of biometric identifier information for profit involving biometric identifier information, with a private right of action as the enforcement mechanism and damages recoverable by the prevailing party. Under the law, "biometric identifier information" means a "physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual, including, but not limited to: (i) a retina or iris scan, (ii) a fingerprint or voiceprint, (iii) a scan of hand or face geometry, or any other identifying characteristic."

Second, the law requires commercial establishments collecting biometric information from customers to disclose this practice through clear and conspicuous signage. The New York City Department of Consumer Affairs has published suggested signage that would be acceptable disclosure.³⁵

Any pending cases should be monitored, as outcomes could impact future interpretations. So far there has only been one case filed, the class action *Rodriguez Perez v. Amazon.com*,³⁶ alleging that Amazon did not properly inform its customers about the use of biometrics at Amazon Go stores, where its "Just Walk Out" technology allows registered customers to make purchases by scanning their palms.

Regarding statewide measures, since 2014 under New York Labor Law, employers are generally prohibited from requiring employers to provide fingerprints as a condition of employment. Additionally, in September 2023 the New York State Department of Education lifted a three-year prohibition on use of any biometrics technology in K-12 school settings after a moratorium and review required in 2020, while continuing a ban on facial recognition technology.³⁷ (See SIA's upcoming guide on state and local laws on facial recognition technology for more information.)

³⁴ <https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCAadmin/0-0-0-42626>

³⁵ <https://www.nyc.gov/assets/dca/downloads/pdf/businesses/Biometric-Identifier-Information-Disclosure-Sign.pdf>

³⁶ <https://www.usatoday.com/story/tech/2023/03/17/amazon-go-lawsuit-biometric-data/11491200002/>

³⁷ <https://www.securityindustry.org/2023/10/02/new-york-lifts-ban-on-biometric-technologies-in-k-12-schools/>

APPENDIX

SAMPLE CONSENT FOR BIPA COMPLIANCE

DISCLAIMER - THIS BIOMETRIC CONSENT FORM HAS BEEN PREPARED AND/OR PROVIDED SOLELY FOR INFORMATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSIDERED OR CONSTRUED AS LEGAL ADVICE ON ANY INDIVIDUAL MATTER OR CIRCUMSTANCE. THE DISTRIBUTION OF THIS CONSENT OR ITS CONTENT IS NOT INTENDED TO CREATE, AND RECEIPT OF IT DOES NOT CONSTITUTE, AN ATTORNEY-CLIENT RELATIONSHIP NOR LEGAL ADVICE OF ANY KIND. THE VIEWS AND OPINIONS EXPRESSED IN THIS CONSENT FORM ARE ONLY INFORMATIONAL AND YOU SHOULD NOT ACT UPON THIS INFORMATION WITHOUT SEEKING LEGAL ADVICE FROM A LAWYER LICENSED IN YOUR JURISDICTION RELATING TO THE TOPICS CONTAINED IN THIS GUIDE. NEITHER DYKEMA, SIA NOR THE AUTHORS ARE RESPONSIBLE FOR ANY ERRORS OR OMISSIONS IN THE CONTENT OF THIS CONSENT OR FOR DAMAGES ARISING FROM THE USE OR UNAUTHORIZED RELIANCE UPON THE CONSENT UNDER ANY CIRCUMSTANCES.

[COMPANY NAME] CONSENT FOR ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT

Biometric Information Privacy Policy

[ABC Company] ("Company") has instituted the following biometric information privacy policy, which includes any and all third party vendors or client(s) where the individual performs work.

Biometric Data Defined

As used in this policy, biometric data includes "biometric identifiers" and "biometric information" as defined in the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq. "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.

Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

Purpose for Collection of Biometric Data

The Company, vendors, third party company, and the licensor of the Company's or Third Party Clients' biometric software will collect, store, and use biometric data solely for [REASON FOR BIOMETRICS], fraud prevention purposes.

Disclosure and Authorization

To the extent that the Company, Third Party Client, and the licensor of the Company's or Third Party Clients' software collect, capture or otherwise obtain biometric data relating to an individual, the Company must:

- a. Inform the employee in writing that the Company, vendor, Third Party Client, and the licensor of the Company's or Third Party Clients' software are collecting, capturing, or

otherwise obtaining the individuals' biometric data, and that the Company is providing such biometric data to its vendors, Third Party Client, and the licensor of the Company's time and attendance software;

- b. Inform the individual in writing of the specific purpose and length of time for which the individual's biometric data is being collected, stored, and used; and
- c. Receive a written release signed by the individual (or his or her legally authorized representative) authorizing the Company and the licensor of the Company's time and attendance software to collect, store, and use the individual's biometric data for the specific purposes disclosed by the Company, and for the Company to provide such biometric data to its vendors and the licensor of the Company's time and attendance software.

The Company, Third Party Client, and the licensor of the Company's or Third Party Clients' time and attendance software will not sell, lease, trade, or otherwise profit from individual's biometric data; provided, however, that the Company's vendors, Third Party Clients, and the licensor of the Company's or Third Party Clients' time and attendance software may be paid for products or services used by the Company that utilize such biometric data.

Disclosure

The Company will not be in possession of the software or the biometric information, but even if the Company becomes in possession of such identifiers or information it will not disclose or disseminate any biometric data to anyone other than its vendors, third party clients where individual is working, and/or the licensor of the Company's time and attendance software providing products and services using biometric data without/unless:

- a. First obtaining written individual consent to such disclosure or dissemination;
- b. The disclosed data completes a financial transaction requested or authorized by the individual;
- c. Disclosure is required by state or federal law or municipal ordinance; or
- d. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

The Company shall retain individual biometric data only until, and shall request that its vendors, Third Party Clients, and/or the licensor of the Company's time and attendance software permanently destroy such data when, the first of the following occurs:

- The initial purpose for collecting or obtaining such biometric data has been satisfied, such as the termination of the individual's employment with the Company, or the individual moves to a role within the Company for which the biometric data is not used; or
- Within 3 years of the individual's last interaction with the Company.

Data Storage

The Company shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic biometric data collected. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which the Company stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as genetic markers, genetic testing information, account numbers, PINs, driver's license numbers and social security numbers.



[COMPANY]

BIOMETRIC INFORMATION CONSENT

[Company] ("Company") is providing this consent form, which individuals must sign as a condition of working at any vendor, third party client site, clients, customers, or other company doing business with Company, which uses biometric software.

The individual named below has been advised and understands that the Company, third party client, and the licensor of the Company's time and attendance software collect, retain, and use biometric data for the purpose of identifying individual s and recording time entries when utilizing the Company's biometric time clocks or time clock attachments. Biometric time clocks are computer-based systems that scan an individual 's finger or other biometrics for purposes of identification. The computer system extracts unique data points and creates a unique mathematical representation used to verify the individual 's identity, for example, when the individual arrives at or departs from the workplace.

The Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq. ("BIPA"), regulates the collection, storage, use, and retention of "biometric identifiers" and "biometric information." "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

The individual understands that he or she is free to decline to provide biometric identifiers and biometric information to the Company, third party client, and the licensor of the Company's time and attendance software without any adverse employment action. The individual may revoke this consent at any time by notifying the Company in writing.

The undersigned individual acknowledges that he/she has received the attached Biometric Information Privacy Policy, and that he/she voluntarily consents to the Company's, third party client, and the licensor of the Company's time and attendance software's collection, storage, and use of biometric data through a biometric time clock, including to the extent that it utilizes the individual's biometric identifiers or biometric information as defined in BIPA, and voluntarily consents to the Company providing or receiving such biometric to its third party client, vendor, third party, and licensor of the Company's software.

Individual Name (print): _____

Individual's signature: _____

Date: _____



securityindustry.org

©2023, Security Industry Association.
All rights reserved.