

# COMPARISON OF STATE BIOMETRIC PRIVACY LAWS

State Laws	<u>Illinois Biometric Information Privacy Act (BIPA)</u>	<u>Texas: Capture or Use of Biometric Identifier Act (CUBI)</u>	<u>Washington: HB 1493</u>	<u>California Consumer Privacy Act of 2018 (CCPA)</u>	<u>New York SHIELD ACT</u>
<b>Definition of Biometric</b>	"Biometric identifier" a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.  "Biometric information" means any information based on an individual's biometric identifier used to identify an individual.	"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.	"Biometric identifier" is data measuring biological characteristics, including fingerprints, voiceprints, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. <b>The definition does not expressly include a record of "hand or face geometry" and excludes physical or digital photograph, video or audio recording.</b>	"Biometric information" means an individual's physiological 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. <b>Broadly defined to future-proof for upcoming biometric technology.</b>	"Biometric information" as defined under private information is data generated by electronic measurements of an individual's unique physical characteristics or digital representation such as a fingerprint, voice print, retina or iris image, or other information used to authenticate or ascertain the individual's identity
<b>Who or what does the law apply to?</b>	A "private entity" (any individual, partnership, corporation, LLC, association, or other group) in possession of biometrics  Does not include a State or local government agency or court or private financial institution	A person capturing a biometric identifier for a commercial purpose  Does not apply to financial institution retaining voiceprint data	A person that enrolls a biometric identifier in a database for a commercial purpose	A business that collects a consumer's personal information	Any person or business which owns or licenses computerized data which includes private information
<b>Are individuals informed of the use of their biometric information?</b>	Yes, written notice is necessary	Yes	Yes, must provide notice	Yes, information may be prominently presented on the homepage of its internet website or in person.	N/A
<b>Must people provide consent prior to capture, storage, or use of their biometrics?</b>	Yes, written consent is necessary	Yes	No, notice is a disclosure that is not considered affirmative consent.	No	N/A
<b>Biometric information must be protected in the same or more protective manner than other data?</b>	Yes	Yes	Yes, as long as reasonable care is given	Yes, as long as reasonable care is given	Yes
<b>Is there an obligation to delete or destroy biometric data?</b>	Yes, a written policy must be made public, establishing a retention schedule and guidelines for permanently destroying biometric data when the initial purpose for collecting or obtaining it has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.	Yes, a person shall destroy the biometric identifier not later than one year after purpose for collecting the identifier expires, or if collected for security purposes by an employer, after termination of employment.	Yes, a person may not retain the biometric information after it is reasonably necessary to comply with law or a court order; protect against fraud, criminal activity, claims, security threats, or liability; and provide the services for which the biometric identifier was enrolled.	Yes, consumers may opt out of having their information sold and have the right to access and delete their personal information.	Yes, within a reasonable amount of time
<b>Must inform in the case of breach?</b>	Illinois law requires expedient notification of a breach	N/A	N/A	N/A	Must provide "notice" in the written form, electronic form, or provide email notice, inform on a webpage and provide information to the media.
<b>Does it create a private right of action?</b>	Yes	Yes	No	Yes	No
<b>What damages may result?</b>	Between \$1,000-\$5,000 or actual damages	Not more than \$25,000 per violation	Not more than \$500,000	Between \$100-\$750 per consumer per incident or actual damages.	N/A