

GLOBAL BIOMETRICS REGULATION CHART

Last Updated: February 2025

Disclaimer: These materials do not constitute legal advice and should not be substituted for the advice of legal counsel.

TABLE OF CONTENTS

California Labor Code § 1051	1
Colorado HB 1130	1
Illinois Biometric Information Privacy Act (BIPA)	2
New York Labor Law § 201-a	2
New York State Education Department Facial Recognition Ban	3
New York City "Commercial Establishments" Ordinance (NYC Commercial Establishments Ordinance).....	3
New York City Tenant Data Privacy Act (TDPA)	4
Portland, Oregon Facial Recognition Ordinance	4
Texas Capture or Use of Biometric Identifiers Act (CUBI)	5
Washington RCW Chapter 19.375 (HB 1493).....	6

GLOBAL BIOMETRICS REGULATION

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
<p><u>California</u></p> <p>California Labor Code § 1051</p> <p>Cal. Lab. Code § 1051</p>	<p><u>Generally</u></p> <p>Employers and related third-party vendors.</p>	<p><u>Fingerprint Data</u></p> <p>Not defined by California Labor Code § 1051.</p>	<p><u>Employers and Vendors</u></p> <ul style="list-style-type: none"> Fingerprint Disclosure Prohibition¹ 	<p><u>Criminal Penalties</u></p> <p>Penalties. Violation constitutes a misdemeanor offense, subject to a fine up to \$1,000 and/or imprisonment up to six months.</p>
<p><u>Colorado</u></p> <p>Colorado HB 1130</p> <p>Effective Date: July 1, 2025</p> <p>C.R.S. § 6-1-1314</p>	<p><u>Controllers</u></p> <p>(1) (a) Conducts business in Colorado; or (b) produces or delivers commercial products or services intentionally targeted to Colorado residents; and (2) processes or controls <i>any</i> amount/volume of biometric identifiers/biometric data.</p> <p><u>Processors</u></p> <p>Person or organization that processes biometric data or biometric identifiers on behalf of controller.</p>	<p><u>Biometric Identifiers</u></p> <p>"Biometric identifier" means data generated by the technological processing, measurement, or analysis of a consumer's biological, physical, or behavioral characteristics, which data can be processed for the purpose of uniquely identifying an individual. 'Biometric identifier' includes: (a) A fingerprint; (b) A voiceprint; (c) A scan or record of an eye retina or iris; (d) A facial map, facial geometry, or facial template; or (e) Other unique biological, physical, or behavioral patterns or characteristics."</p>	<p><u>Controllers</u></p> <ul style="list-style-type: none"> Consent Notice Privacy Policy Data Retention and Destruction Disclosure Limitation Transactional Prohibition Data Security Biometric Data Assessment² Security Incident Response Program Purpose Specification Data Minimization Use/Purpose Limitation Data Subject Rights Compliance Employment-Specific Requirements and Limitations 	<p><u>Regulatory Enforcement Authority.</u> The Colorado AG and district attorneys have authority to enforce the Colorado Privacy Act (CPA).</p> <p>Remedies. (1) Civil penalties up to \$20,000 per violation under Colorado UDAP; (2) disgorgement; (3) restitution; (4) attorney's fees and costs; and (5) injunctive relief.</p>

¹ California Labor Code § 1051 prohibits employers from obtaining current or prospective employee fingerprint data and then "furnishing" or sharing such data with third parties. The California AG has clarified that no violation of § 1051 occurs where the disclosure of fingerprint data satisfies two criteria: (1) disclosure is made solely to a third party acting as the employer's agent and for the employer's exclusive benefit; and (2) fingerprint data is not further furnished or disclosed by either employer or agent.

² Colorado HB 1130 obligates controllers to conduct review at least once annually to evaluate whether storage of biometric data is no longer necessary, adequate, or relevant to express processing purpose(s) disclosed at initial time of collection; where biometric data is no longer necessary, adequate, or relevant, data must be deleted at "earliest reasonably feasible date," but no more than 45 days after date of determination.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
		<p><u>Biometric Data</u></p> <p>"Biometric data' means one or more 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."</p>	<p><u>Processors</u></p> <ul style="list-style-type: none"> • Data Security • Security Incident Response Program • Employment-Specific Requirements and Limitations 	
<p><u>Illinois</u></p> <p>Illinois Biometric Information Privacy Act (BIPA)</p> <p>740 ILCS 14/1, <i>et seq.</i></p>	<p><u>Generally</u></p> <p>"Private entities" that collect or process "biometric identifiers" or "biometric information."</p> <p><u>Private Entities</u></p> <p>"Any individual, partnership, corporation, limited liability company, association, or other group, however organized."</p>	<p><u>Biometric Identifiers</u></p> <p>"Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."</p> <p><u>Biometric Information</u></p> <p>"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."</p>	<p><u>Private Entities</u></p> <ul style="list-style-type: none"> • Consent • Notice • Privacy Policy • Data Retention and Destruction • Disclosure Limitation • Transactional Prohibition • Data Security 	<p><u>Private Right of Action</u></p> <p>Private Right of Action. Any person "aggrieved" by BIPA violation has right of action against offending party (actual injury/damage not required).</p> <p>Damages. (1) Statutory damages of: (a) \$1,000 per negligent violation; or (b) \$5,000 per reckless/intentional violation; (2) attorney's fees and costs; and (3) injunctive relief.</p>
<p><u>New York</u></p> <p>New York Labor Law § 201-a</p> <p>N.Y. Lab. Law § 201-a</p>	<p><u>Generally</u></p> <p>Employers and related third-party vendors.</p>	<p><u>Fingerprint Data</u></p> <p>Not defined by Labor Law § 201-a.</p>	<p><u>Employers and Vendors</u></p> <ul style="list-style-type: none"> • Prohibition on Mandatory Fingerprinting of Employees or Job Applicants³ 	<p><u>Criminal Penalties</u></p> <p>Penalties. Violation constitutes misdemeanor offense; first violation subject to a fine up to \$100; second violation subject to a fine between \$100 to \$500, imprisonment up to 30 days, or both; subsequent violations subject to a</p>

³ New York Labor Law § 201-a prohibits employers from requiring employees to be fingerprinted as condition of securing or continuing employment. The New York State Department of Labor (NYDOL) has clarified that it is the initial act of fingerprinting, rather than subsequent use or storage of fingerprints, which is prohibited. Thus, mandatory use of a biometric timekeeping device, for example, violates Labor Law § 201-a. With that said, *voluntary* fingerprinting of employees *is* permissible under Labor Law § 201-a.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
				minimum fine of \$300, imprisonment up to 60 days, or both.
<p><u>New York</u></p> <p>New York State Education Department Facial Recognition Ban</p> <p>N.Y. Tech. Law § 106-b</p>	<p><u>Generally</u></p> <p>Use of "facial recognition technology" or "facial recognition" by New York "Schools."</p> <p><u>Facial Recognition/Facial Recognition Technology</u></p> <p>Tool using an automated or semi-automated process that assists in uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's face.</p> <p><u>Schools</u></p> <p>New York public or nonpublic elementary schools, secondary schools, and charter schools.</p>	<p><u>Biometric Information</u></p> <p>"Biometric information" means physical, physiological, or behavioral characteristics that are attributable to a person, including but not limited to facial characteristics, fingerprint characteristics, eye characteristics, vocal characteristics, and any other characteristics that can be used to identify a person including, but not limited to: fingerprints; handprints; retina and iris patterns; DNA sequence; voice; gait; and facial geometry."</p>	<p><u>Schools</u></p> <ul style="list-style-type: none"> Facial Recognition Technology Prohibition 	<p><u>Regulatory Enforcement Authority.</u> The New York State Commissioner of Education has authority to enforce N.Y. Tech. Law § 106-b.</p> <p><u>Remedies.</u> Withholding of public funding from School.</p>
<p><u>New York City</u></p> <p>New York City "Commercial Establishments" Ordinance (NYC Commercial Establishments Ordinance)</p>	<p><u>Generally</u></p> <p>"Commercial establishments" that process "biometric identifier information."</p> <p><u>Commercial Establishments</u></p> <p>"A place of entertainment, a retail store, or a food and drink establishment."</p>	<p><u>Biometric Identifier Information</u></p> <p>"The term '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</p>	<p><u>Commercial Establishments</u></p> <ul style="list-style-type: none"> Public Signage Notice⁴ Transactional Prohibition 	<p><u>Private Right of Action</u></p> <p><u>Private Right of Action.</u> Any person "aggrieved" by violation may commence action against offending party.</p> <p><u>Damages.</u> (1) Statutory damages of: (a) \$500 per notice requirement violation; (b) \$500 per negligent</p>

⁴ NYC Commercial Establishments Ordinance requires posting of "clear and conspicuous signage" near all customer entrances providing notice of collection, retention, storage, or sharing (as applicable) of biometric data.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
N.Y.C. Admin. Code § 22-1201, <i>et seq.</i>		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."		transactional prohibition violation; and (c) \$5,000 per reckless or intentional transactional prohibition violation; (2) attorney's fees and costs; and (3) injunctive relief.
<p><u>New York City</u></p> <p>New York City Tenant Data Privacy Act (TDPA)</p> <p>N.Y.C. Admin. Code § 26-3001, <i>et seq.</i></p>	<p><u>Generally</u> Owners and operators of "smart access buildings" that utilize "smart access systems" which process "biometric identifier information."</p> <p><u>Smart Access Buildings</u> Building or structure used as home or residence that is rented, leased, or otherwise occupied by three or more families living independent of each other.</p> <p><u>Smart Access Systems</u> System that uses biometric identifier information (or other digital technology) grant entry to smart access building, common areas, or individual dwelling units.</p>	<p><u>Biometric Identifier Information</u> "The term 'biometric identifier information' means a physiological, biological or behavioral characteristic that is used to identify, or assist in identifying, an individual, including, but not limited to: (i) a retina or iris scan; (ii) a fingerprint; (iii) a voiceprint; (iv) a scan or record of a palm, hand or face geometry; (v) gait or movement patterns; or (vi) any other similar identifying characteristic."</p>	<p><u>Smart Access Building Owners and Operators</u></p> <ul style="list-style-type: none"> • Consent • Privacy Policy • Data Retention and Destruction • Disclosure Limitation • Transactional Limitation • Data Security • Data Minimization • Use/Purpose Limitation 	<p><u>Private Right of Action</u> Private Right of Action. Any dwelling occupant has the right to bring civil action for violation of TDPA disclosure or transactional limitations.</p> <p>Damages. (1) Statutory damages between \$200 to \$1,000 per violation of disclosure or transactional limitations; and (2) attorney's fees and costs.</p>
<p><u>Portland, Oregon</u></p> <p>Portland, Oregon Facial Recognition Ordinance</p>	<p><u>Generally</u> "Private entities" that use "face recognition technologies" in places of public accommodation within</p>	N/A	<p><u>Private Entities</u></p> <ul style="list-style-type: none"> • Face Recognition Technologies Prohibition⁵ 	<p><u>Private Right of Action</u> Private Right of Action. Any person "injured by a material violation" of ordinance has cause of</p>

⁵ Portland Facial Recognition Ordinance prohibits use of face recognition technologies in places of public accommodation within boundaries of city of Portland.

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
Portland, Or. City Code Ch. 34.10	<p>boundaries of the City of Portland.</p> <p><u>Private Entities</u> "Any individual, sole proprietorship, partnership, corporation, limited liability company, association, or any other legal entity, however organized."</p> <p><u>Face Recognition Technologies</u> "Automated or semi-automated processes using face recognition that assist in identifying, verifying, detecting, or characterizing facial features of an individual or capturing information about an individual based on an individual's face."</p> <p><u>Face Recognition</u> "Automated searching for a reference image in an image repository by comparing the facial features of a probe image with the features of images contained in an image repository (one-to-many search)."</p>			<p>action against non-compliant entity.</p> <p>Damages. (1) Statutory damages of \$1,000 per day of violation; and (2) attorney's fees.</p>
<p><u>Texas</u></p> <p>Texas Capture or Use of Biometric</p>	<p><u>Generally</u></p> <p>"Persons" that capture or collect "biometric identifiers" for a commercial purpose.</p>	<p><u>Biometric Identifiers</u></p> <p>"[B]iometric identifier" means a retina or iris scan, fingerprint, voiceprint, or</p>	<p><u>Persons</u></p> <ul style="list-style-type: none"> • Consent • Notice • Data Retention and Destruction 	<p><u>Regulatory Enforcement Authority.</u> The Texas AG has authority to enforce CUBI.</p>

Law	Applicability	Covered Data	Compliance Obligations	Enforcement
Identifiers Act (CUBI) Tex. Bus. & Com. Code § 503.001	<u>Persons</u> Not defined by CUBI.	record of hand or face geometry."	<ul style="list-style-type: none"> • Disclosure Limitation • Transactional Limitation • Data Security 	Remedies. Civil penalties of up to \$25,000 per violation.
<u>Washington</u> Washington RCW Chapter 19.375 (HB 1493) Wash. Rev. Code § 19.375.010, <i>et seq.</i>	<u>Generally</u> "Persons" who capture or enroll a "biometric identifier" for a commercial purpose. <u>Persons</u> "An individual, partnership, corporation, limited liability, company, organization, association, or any other legal or commercial entity."	<u>Biometric Identifiers</u> "Biometric identifier" 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."	<u>Persons</u> <ul style="list-style-type: none"> • Consent • Notice • Data Retention and Destruction • Disclosure Limitation • Transactional Limitation • Data Security • Use/Purpose Limitation • Mechanism to Prevent Subsequent Use of Biometric Data⁶ 	<u>Regulatory Enforcement Authority.</u> The Washington AG has authority to enforce HB 1493. Remedies. (1) Civil penalties up to \$7,500 per violation under Washington Consumer Protection Act (Washington UDAP); (2) disgorgement; (3) restitution; (4) attorney's fees and costs; and (5) injunctive relief.

⁶ Washington HB 1493 requires implementation of mechanism to prevent subsequent use of biometric data; must be in place prior to collection of biometric data.