California Biometric Information Privacy Act

Summary

This Act seeks to regulate the capture, processing, storage, and transfer of biometric data by private commercial entities. Individuals must be notified about the collection, storage, and distribution of their biometric data, and private commercial entities must obtain an individual's express affirmative consent except in limited instances of shoplifter identification and targeted advertising. After the biometric data is no longer relevant to a private commercial entity's service, the company must take appropriate steps to erase the stored data. This Act creates penalties for violating these rules, based on historical penalties for identity theft documented by the US Department of Justice in 2014. This Act draws salient language from Texas Code Ann. § 503.001 (Capture or Use of Biometric Identifier) and Illinois Comp. Stat. § 740, 14/5 (Biometric Information Privacy Act).

SECTION 1. SHORT TITLE. This Act may be cited to as the California Biometric Information Privacy Act of 2017 or CalBIPA.

SECTION 2. DEFINITIONS. For the purposes of this Act, the following definitions apply:

(1) “Biometric Information” includes, but is not limited to, any information captured directly or derived from a retina or iris scan, fingerprint, voiceprint, scan of hand or face geometry, or a scan of bone structure or gait. Biometric information does not include writing samples, written signatures, 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.

(2) "Biometric Identification" refers to the use of biometric information to identify specific individuals.

(3) "Biometric Characterization" refers to the use of biometric information to classify individuals according to shared traits.

(4) "Collection Limitation" refers to minimizing the capture and storage of information to what is necessary for service provision described in a Notice.

(5) "Express Affirmative Consent" refers to written consent provided for only the specific uses of information described in a Notice.

(6) "Facial Recognition Technology" refers to the hardware, software, algorithms, and techniques used to identify faces in photos, videos, or other visual material and link faces to personally identifiable information.

(7) “Notice” refers to a conspicuous attempt to alert individuals whose biometric information is being captured, stored, processed, or transferred about the details of the

acquisition and use of such information.

(8) “Private Entity” refers to any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency nor does it include any court of California, a clerk of the court, or a judge or justice thereof.

(9) “Vital Everyday Services” refer to services that are essential to an individual’s ordinary course of business including, but not limited to, accessing financial records or personal email.

SECTION 3. SCOPE; EXCEPTIONS.

(a) Scope. This act applies to private entities that capture, process, store, or transfer biometric information.

(b) Exceptions.

(1) This act does not apply to private entities whose business is data transfer or storage and who do not provide any products or services specific to biometric information. This includes mobile phone service providers, Internet service providers, CCTV operators, or data storage providers, who may incidentally store or transfer biometric information.

(2) This act does not apply to private entities providing biometric information to government entities if:

(i) Pursuant to a warrant, express affirmative consent, or emergency as set out by California Penal Code Section 1546 (CalECPA). Government entities must follow any applicable notice provisions in CalECPA.

(ii) Pursuant to a search for a missing person, as set out by California

Penal Code Section 14205, where there is strong reason to believe the missing person might be found by accessing the private entity's database of stored biometric information.

SECTION 4. RULES.

(a) A private entity shall not capture, process, use, store, or transfer an individual's biometric information for a commercial purpose unless the private entity:

(1) provides notice to the individual; and

(2) obtains the individual's express affirmative consent.

(b) A private entity shall not use biometric information for purposes other than for what they have received express affirmative consent.

(c) An individual may revoke consent to any capture, process, use, store, or transfer of the individual's biometric information at any time.

(d) A private entity in possession of biometric information must:

(1) store all biometric information in a reasonably secure manner as outlined in California Civil Code Section 1798.81.5(b).

(2) permanently destroy the biometric information within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the information expires, except where:

(i) biometric information captured for a commercial purpose is used in connection with an instrument or document that is required by another law to be maintained for a period longer than one year, the private entity who possesses the biometric information shall destroy the information within a reasonable time, but not later than the first anniversary of the

date the instrument or document is no longer required to be maintained by law.

(ii) biometric information captured for a commercial purpose is collected for security purposes by an employer, the purpose for collecting the biometric information is presumed to expire on termination of the employer relationship.

(3) develop a written policy, made available to the public, that establishes a retention schedule and guidelines for permanently destroying biometric information.

(e) A private entity shall destroy within a reasonable timeframe, not longer than a month, any stored copies of biometric information at the request of individuals whose biometric information has been captured or stored by them, except in cases outlined in Subsections (d)(2)(i) and (ii).

(f) A private entity shall audit its biometric information systems yearly, and the audits must:

(1) demonstrate that the entity's systems practice reasonable collection limitation;

(2) demonstrate that the entity's systems perform with reasonable levels of accuracy and precision; and

(3) demonstrate that the entity's systems reasonably limit inaccuracies that may create a discriminatory impact for individuals under the protected categories outlined in California Civil Code Section 51.

(g) A private entity must make audit results of the biometric systems they have released in the market publicly available. Tests of unreleased biometric systems are exempt from the publication requirement until they enter the market, at which point an approved audit must be conducted and published

(h) A private entity's audit tests and associated test datasets must be approved by the

California Department of Consumer Affairs.

(i) A private entity shall maintain records of any internal or independent tests or audits of the security, privacy, or performance of their systems that are currently in the market.

(j) A private entity may capture, process, and transfer biometric information in real-time for the purpose of identifying shoplifters after notice and without consent.

(1) Biometric information captured, processed, or transferred for the purpose of identifying shoplifters cannot be used for any other purpose.

(2) Only individuals who have been previously convicted of crimes as defined in California Penal Code Section 459.5 may have their biometric information added to shoplifter identification databases.

(k) A private entity that captures, uses, or transfers biometric information in real-time for targeted advertising as a result of biometric identification is governed by all above subsections.

(l) A privacy entity that captures, uses, or transfers biometric information in real-time for targeted advertising as a result of biometric characterization is governed by all above subsections, except as superseded by the following:

(1) Biometric information may be captured, processed, or transferred in real-time for targeted advertising after notice and without consent.

(2) Biometric information cannot be stored permanently without express affirmative consent.

(3) Biometric information cannot be used for targeted advertising that promotes pharmaceuticals, supplements, reproductive health, child-rearing, and any other products that could be recommended on the basis of a perceived medical condition.

(m) Where access to vital everyday services is involved, there must be an alternate option

available to individuals who do not wish to use biometric information for authentication.

SECTION 5. ENFORCEMENT; PENALTIES.

(a) Any individual aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

(1) against a private entity that negligently violates a provision of this Act, liquidated damages of $2,000 or actual damages, whichever is greater;

(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $7,500 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate.

(b) The attorney general may bring an action to recover the civil penalty.

SECTION 6. SEVERABILITY. The provisions of this Act are severable. If any provision of this Act or its application is held invalid, that invalidity shall not affect any other provision or application that can be given effect without the invalid provision or application.

SECTION 7. EFFECTIVE DATE. This Act will be effective as of May 5, 2017.

Model law sources:
Texas Code Ann. § 503.001 (Capture or Use of Biometric Identifier)
Illinois Comp. Stat. § 740, 14/5 (Biometric Information Privacy Act)