State Biometric Identifiers Privacy Act[1]

Section 1. Short title. This Act may be cited as the Biometric Identifiers Privacy Act (BIPA).

Section 2. Legislative findings; intent. The [NAME OF LEGISLATIVE BODY] finds all of the following:

(A) Businesses are increasingly using biometrics to attempt to verify customer identity, streamline transactions, control access to secure areas, and maximize revenues.

(B) Biometrics are unlike other unique identifiers that are used to verify identity or access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(C) The public has grown wary of the use of biometrics because of concerns about the security of protecting such information once it is captured and stored without their consent. Indeed, recent data breaches have exposed people's biometric identifiers, leaving people vulnerable to harm.

(D) Additionally, biometric identifiers can be collected without people's knowledge, applied instantaneously to identify people in circumstances where they have an expectation of privacy and anonymity, and used to identify and track people's movements, activities, and associations.

[1] This model bill is based upon the Illinois Biometric Information Privacy Act (IL-BIPA), with some provisions based on Texas' and Washington State's biometric privacy laws and the California Consumer Privacy Act, as well as related legislative efforts in Maryland and Maine. Significant differences between IL-BIPA and this model bill are noted and explained in the footnotes (which are not intended to be part of the text of the bill).

(E) Studies have also shown that one increasingly prevalent biometric collection and matching technology, facial recognition technology, has worse misidentification/misclassification rates when used on faces of color, of women, of children, of the elderly, and of transgender and non-binary persons. This has led to documented cases of businesses refusing admission or service to people because facial recognition systems incorrectly "matched" them to photos of suspected shoplifters or others who had been barred from the premises.

(F) The lack of legal protections regulating the collection, use, safeguarding, and storage of biometrics means that many members of the public fear that their biometric identifiers may be collected and used without their knowledge and consent.

(G) The full ramifications of biometric technology are not fully known.

(H) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers.

Section 3. Definitions. In this Act:

(A) "Biometric Identifier"[2] means the data of an individual generated by measurements of an individual's unique biological characteristics such as a faceprint, fingerprint, voiceprint, retina or iris image, or any other biological characteristic that can be used to uniquely identify the individual.

(1) "Biometric identifier" does not include:

(a) A writing sample of written signature;

[2] This more thorough and "evergreen" definition of "biometric identifier" was needed because the 10+ year old IL-BIPA definition has become dated. The definition of "biometric information" that appears in IL-BIPA, and all references thereto in the bill, was deleted to avoid potential First Amendment issues. This updated definition is largely drawn from the Washington State biometric identifiers privacy law, which was enacted in 2017.

(b) A photograph or video, except[3] "biometric identifier" includes data generated, captured, or collected from the biological characteristics of a person depicted in a photograph or video;

(c) A human biological sample used for valid scientific testing or screening;

(d) Demographic data;

(e) A physical description, including height, weight, hair color, eye color, or a tattoo description;

(f) Any donated portion of a human body stored on behalf of a recipient of potential recipient of a living cadaveric transplant and obtained or stored by a federally designated organ procurement agency, including an organ, tissue, an eye, a bone, an artery, blood, and any other fluid or serum;

(g) Information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountably Act of 1996;

(h) Any image or film of the human anatomy used to diagnose, provide a prognosis for, or treat an illness or other medical condition or to further validate scientific testing or screening including an x-ray, a roentgen process, computed tomography, a magnetic resonance imaging image, a positron emission tomography scan, and mammography; or

(i) Information collected, used, or disclosed for human subject research that is conducted in accordance with the federal policy for the protection of human subjects, 45 C.F.R. Part 46, or other similar

[3] This clarification was made to preempt arguments that companies have tried to make in Illinois, where they argued that the photographs exemption from the definition of "biometric identifier" means that biometric identifiers are only covered if they are collected in-person, and are not covered if they are collected from a photo of a person. Companies have lost this argument in every court case we are aware of, so the threat is not great, but it would be best to avoid the interpretive fight in the first place.

research ethics laws, or with the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use.

(B) "Private entity" means any individual acting in a commercial context, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency or entity.

(C) "Verified request" means a request that is made by a person or by an individual authorized to act as that person's representative, and that the private entity can verify, using commercially reasonable methods, to be the person whose biometric identifier(s) the private entity collected.

(D) "Written release" means informed written consent, including written consent provided by electronic means. A valid written release may not be secured through a general release or user agreement.

(1) In the context of employment, a written release:

(a) May only be used[4] to secure consent to collect and use biometric identifiers for the purposes of:

(i) Permitting access to secure physical locations and secure electronic hardware and software applications, without retaining data that allows for employee location tracking or the tracking of how long an employee spends using a hardware or software application; or

(ii) Recording the commencement and conclusion of an employee's full work day and meal/rest breaks in excess of 30 minutes;

(b) May be secured in the form of a written release executed by an employee as a condition of employment.

Section 4. Retention; collection; disclosure; destruction.

[4] IL-BIPA provides for any use as a condition of employment, but that could lead to the constant monitoring of employees at work. Additionally, employees almost always have unequal bargaining power vis-à-vis their employers, and that makes a broader reliance on consent ineffective. This strikes a better, less-Orwellian balance.

(A) (1) A private entity in possession of biometric identifiers must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying a biometric identifier of an individual on the earliest of:

(a) The date on which the initial purpose for collecting or obtaining the biometric identifier has been satisfied;

(b) One year[5] after the individual's last interaction with the private entity; or

(c) 30 days after receiving a verified request to delete the biometric identifiers submitted by the individual or the individual's representative.[6]

(2) Absent a valid warrant or subpoena issued by a court of competent jurisdiction, or a compulsory request or demand issued by a state agency in an investigation of a violation of this Chapter, a private entity in possession of biometric identifiers must comply with its established retention schedule and destruction guidelines.

(3) A private entity is not required[7] to make available to the public a written policy that:

(a) Applies only to employees of that private entity; and

(b) Is used solely within the private entity for operation of the private entity.

(B) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's biometric identifier, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier is being collected or stored;

---

[5] Reduced from 3 years in IL-BIPA, which is an unnecessarily long period of time. This mirrors the Texas Capture or Use of Biometric Identifiers Act, which has a similar 1-year retention period.
[6] This consumer empowering "right to request deletion" is not found in IL-BIPA. This mirrors the California Consumer Privacy Act, which has a similar provision.
[7] This addition, which was in the 2022 BIPA bills from Maine and Maryland, was added as a reasonable accommodation to businesses that are worried about their exposure to lawsuit damages for technical violations of the statute that do not result in harm.

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or the subject's legally authorized representative.

(C) No private entity that collects a person's biometric identifier may:

(1) Sell, lease, or trade that biometric identifier; or

(2) Permit any entity to which a biometric identifier is transferred, shared, or provided to sell, lease, or trade that biometric identifier.

(D) No private entity that collects a biometric identifier may disclose, redisclose, or otherwise disseminate a person's biometric identifier unless:

(1) the subject of the biometric identifier or the subject's legally authorized representative executes a written release consenting to the specific disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction, or a compulsory request or demand issued by a state agency in an investigation of a violation of this Chapter.

(E) A private entity may not[8]:

(1) Condition the provision of a good or service on the collection, use, disclosure, transfer, sale, retention, or processing of biometric identifiers unless biometric identifiers are strictly necessary to provide the good or service; or

[8] This subsection was added to protect the ability of individuals to exercise their rights under this bill free from coercion. This mirrors the California Consumer Privacy Act, which has a similar provision.

(2) Charge different prices or rates for goods or services or provide a different level of quality of a good or service to any individual who exercises the individual's rights under this subtitle.

(F) A private entity in possession of a biometric identifier shall:

(1) store, transmit, and protect from disclosure all biometric identifiers using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

Section 5. Right To Know.

(A) At the request of an individual or an individual's legally authorized representative, a private entity that collects biometric identifiers shall disclose to the individual, free of charge, the individual's biometric identifier and information related to the use of the biometric identifier, including:

(1) The precise type of biometric identifiers that were collected and/or used;

(2) The specific sources from which the private entity collected the biometric identifiers;

(3) The specific purpose for which the private entity used the biometric identifiers and personal information;

(4) The identities of third parties with whom the private entity shares the biometric identifiers and the purposes of sharing; and

(5) The specific biometric identifiers that the business discloses to third parties.

(B) The requirements of Section 5 shall only apply to[9]:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that (i) does business in the State of [STATE NAME], (ii) is organized or operated for the financial benefit of its shareholders or other owners, (iii) collects consumers' biometric identifiers or

[9] This limitation is styled after the California Consumer Protection Act.

has such identifiers collected on its behalf, and (iv) had annual gross revenues in excess of ten million dollars ($10,000,000) in the preceding calendar year.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers' personal information. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned.

(3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

Section 6. Right of action; enforcement.

(A) An individual alleging a violation of this subtitle[10] may bring a civil action against the offending private entity in a court of competent jurisdiction. A prevailing plaintiff[11] may recover for each violation:

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

[10] This is a change from IL-BIPA's "aggrieved party" language that had to be litigated to clarify that the person didn't have to prove actual damages. This new language clears up that ambiguity.
[11] Changed from "party" to avoid threat of defendants seeking legal fees from plaintiffs, the risk of which would likely discourage parties with legitimate claims from taking action.

(2) Against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 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 or declaration, as the court may deem appropriate.

(B) The Attorney General of [STATE NAME] may bring an action against a private entity who violates any provisions of this Act, and shall be entitled to seek any forms of relief and remedies available to private plaintiffs, including the collection of damages as a civil penalty.

Section 7. Construction.

(A) Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers in any action of any kind in any court, or before any tribunal, board, or agency.

(B) Nothing in this Act shall be construed to conflict with the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under that Act.

(C) Nothing in this Act shall be deemed to apply in any manner to information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.

(D) Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government, and such exemption shall only apply to the extent the collection, retention, and use of the biometric identifier is in direct service of the purpose for which the State agency or local unit of government retained the services of the contractor, subcontractor, or agent.

Section 8. Severability. The provisions in this Act are severable. If any part or provision of this Act, or the application of this Act to any person or circumstance, is

held invalid, the remainder of this Act, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Section 9. Effective date. This Act takes effect 180 days after becoming law.