HOUSE DOCKET, NO. 3053 FILED ON: 1/20/2023

HOUSE . . . . . No. 63

The Commonwealth of Massachusetts

PRESENTED BY:

Dylan A. Fernandes

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act to protect biometric information.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
Dylan A. Fernandes	*Barnstable, Dukes and Nantucket*	*1/19/2023*
Mindy Domb	*3rd Hampshire*	*1/23/2023*
Bud L. Williams	*11th Hampden*	*2/6/2023*

HOUSE DOCKET, NO. 3053 FILED ON: 1/20/2023

HOUSE . . . . . No. 63

By Representative Fernandes of Falmouth, a petition (accompanied by bill, House, No. 63) of Dylan A. Fernandes, Mindy Domb and Bud L. Williams for legislation to protect biometric information. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Third General Court
(2023-2024)

An Act to protect biometric information.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The General Laws, as appearing in the 2020 Official Edition, are hereby amended by inserting after chapter 93L the following chapter:

CHAPTER 93M. Privacy Protections for Biometric Information

Section 1. Definitions

a. As used in this chapter, the following words shall, unless the context clearly requires otherwise, have the following meanings:—

1. "Biometric information" or "biometric data" means information or data that pertains to measurable biological or behavioral characteristics of an individual that can be used singularly, or in combination with each other, or with other information, for verification, recognition, or identification of an unknown individual. Examples include but are not limited to

fingerprints, retina and iris patterns, voiceprints, D.N.A. sequences, facial characteristics and face geometry, gait, handwriting, keystroke dynamics, and mouse movements.

Biometric information does not include writing samples, written signatures, mere 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 information does not include donated organs, tissues, parts of the human body, blood, or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants obtained or stored by a federally designated organ procurement agency.

Biometric information does not include information captured from a patient by a health care provider or health care facility, or collected, processed, used, or stored exclusively for medical education or research, public health or epidemiological purposes, health care treatment, health insurance, payment, or operations, so long as such information is protected under the federal Health Insurance Portability and Accountability Act of 1996 and applicable federal and state laws and regulations.

Biometric information does not include information captured from an X-ray, roentgen process, computed tomography, M.R.I., P.E.T. scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

2. “Biometric Privacy Policy” means the policies, practices, and procedures that covered entities abide by regarding the collection, processing, management, storage, retention, and deletion of biometric information.

3. “Collect” means to obtain, generate, create, receive, or access biometric information.

4. “Consent” means freely given, specific, informed, unambiguous, opt-in consent.

5. “Covered entity” means any individual, partnership, corporation, limited liability company, association, or another group, however organized. A covered entity does not include a state or local government agency, or any court of Massachusetts, a clerk of the court, or a judge or justice thereof.

6. “Data processor” means a person or entity that processes biometric information on behalf of a covered entity.

7. “Disclose” means to make biometric information available to a covered entity, data processor, or person, intentionally or unintentionally, including but not limited to by sharing, publishing, releasing, transferring, disseminating, providing access to, failing to restrict access to, or otherwise communicating such biometric information orally, in writing, electronically, or by any other means.

8. “Harm” means potential or realized adverse consequences to an individual, including but not limited to:—

i. Direct or indirect financial harm;

ii. Physical harm or threats to individuals or property;

iii. Interference with or surveillance of First Amendment-protected activities;

iv. Interference with the right to vote or with free and fair elections;

v. Loss of individual control over biometric information via non-consensual collection, processing, sharing, or disclosure of biometric information, data breach, or other actions that violate this chapter;

vi. Other effects that are foreseeable to, or contemplated by, a covered entity.

9. "Individual" means a person located in the Commonwealth of Massachusetts.

10. "Monetize" means to disclose an individual's biometric information for profit or in exchange for monetary or other consideration. This term includes but is not limited to selling, renting, trading, or leasing biometric information.

11. "Person" means any natural person.

12. "Process" means to perform any action or set of actions on or with biometric information, including but not limited to collecting, accessing, using, storing, retaining, sharing, monetizing, analyzing, creating, generating, aggregating, altering, correlating, operating on, recording, modifying, organizing, structuring, disclosing, transmitting, selling, licensing, disposing of, destroying, de-identifying, or otherwise manipulating biometric information.

13. "Identification" and "recognition" means the use of automated systems to compare the biometric information of an individual with biometric information available in a specific database (i.e., a 1-to-n matching system where "n" is the total number of biometric data points in a database) to attempt to ascertain the identity of an individual.

14. "Reasonably understandable" means of length and complexity such that an individual with an eighth-grade reading level, as established by the department of education, can read and comprehend.

15. “Third party” means any covered entity, person, data processor, or governmental entity other than (i) a covered entity or a data processor that collected or processed biometric information in accordance with this chapter or (ii) the individual to whom the biometric information pertains.

16. “Use model” means a discrete purpose for which collected biometric information is to be processed, including but not limited to first-party marketing, third party marketing, first-party research and development, third party research and development, and product improvement and development.

17. “Verification” means the use of automated systems to compare the biometric information of an individual with that individual’s biometric information already existing in a database (i.e., 1-to-1 matching systems) to confirm or verify the identity of such individual.

Section 2. Protection of biometric information

a. A covered entity or data processor shall not collect or process an individual’s biometric information for identification purposes unless it first:—

1. informs the individual in writing in a way that the individual can reasonably understand that the covered entity is going to collect and process biometric information;

2. provides the individual with the Biometric Privacy Policy; and

3. obtains explicit non-electronic, handwritten consent, executed by the individual or their legal guardian or representative, that authorizes the collection and processing of biometric information for a specific purpose, excluding monetization. Such consent shall be delivered to the covered entity by hand, postal mail, facsimile, or via email with an electronic scan attached.

b. A covered entity or data processor shall not collect or process an individual's biometric information for verification purposes unless it first:—

1. informs the individual in writing in a way that the individual can reasonably understand that the covered entity is going to collect and process biometric information;

2. provides the individual with the Biometric Privacy Policy; and

3. obtains explicit handwritten or electronic consent from the individual or their legal guardian or representative before any such information is collected or processed.

c. Consent provided under the previous paragraphs shall expire after three years or when the initial purpose for processing the biometric information has been satisfied, whichever occurs first, provided that such consent may be renewed pursuant to the same procedures. Upon expiration, any biometric information possessed by a covered entity must be permanently destroyed.

d. A covered entity shall always maintain and make available to the individual a Biometric Privacy Policy, which shall include, at a minimum, the following:—

1. the use models, detailing whether the biometric information is going to be used for identification or verification purposes;

2. all data management and data security policies governing biometric information;

3. all disclosure practices; and

4. the retention schedule and guidelines for permanently deleting biometric information.

e. A covered entity shall provide notice of any change to its Biometric Privacy Policy at least 20 business days before the change goes into effect and shall newly request consent pursuant to subsections (a) and (b).

f. A covered entity in possession of biometric information shall:

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

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

g. A covered entity, data processor, or third party in lawful possession of biometric information shall not disclose, cause to disclose, or otherwise disseminate or cause to disseminate an individual's biometric information unless the disclosure is:—

1. required for the provision of a service or product by the covered entity and the individual provides consent in accordance with paragraphs (a) or (b);

2. necessary to complete a financial or commercial transaction requested by the individual and the individual provides consent in accordance with paragraph (a) or (b);

3. for a single purpose, to a specific third party, and authorized pursuant to a separate handwritten consent from that required under paragraphs (a) and (b), sent to the covered entity by postal mail, facsimile, or electronic mail attached with electronic scan;

4. routinely required by state or federal law, in which case the individual must be given adequate notice in the Biometric Privacy Policy;

5. required pursuant to a valid warrant issued by a court of competent jurisdiction; or

6. necessary to respond to an emergency service agency responding to a 911 communication or any other communication reporting an imminent threat to life or property.

h. It is unlawful for a covered entity, data processor, or third party to monetize an individual's biometric information.

Section 3. Notice of disclosure

a. When a covered entity, its affiliated data processors, or the third parties they contracted with disclose or share biometric information pursuant to a valid warrant issued by a court of competent jurisdiction, the covered entity, data processor, or third party receiving such warrant shall serve or deliver the following information to the individual to which the warrant request biometric information refers by registered or first-class mail, electronic mail, or other means reasonably believed to be effective:—

1. A copy of the warrant and a notice that informs the individual of the nature of the inquiry with reasonable specificity;

2. That biometric information related to the individual was supplied to, or requested by, a requesting entity and the date on which the supplying or request took place;

3. An inventory of the biometric information requested or supplied;

4. Whether the information was in possession of the covered entity, an affiliate data processor, or another third party; and

5. The identity of the person that sought the warrant from the court, if known.

b. The covered entity, data processor, or third party shall immediately serve or deliver such notification upon receiving a warrant requesting or compelling the disclosure of biometric information.

c. Notwithstanding the previous paragraphs, a government entity may apply to the court for an order delaying such notification. The court may issue the order if the notification of the existence of the legal request will result in danger to the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, or intimidation of potential witnesses, or otherwise seriously jeopardize an investigation or unduly delay a trial. If granted, such an order shall not exceed 30 days but may be renewed for up to 30 days at a time while grounds for the delay persist.

d. Covered entities shall take all reasonable measures and engage in all legal actions available to ensure that warrants requesting or compelling the disclosure of biometric information are valid under applicable laws and statutes.

Section 4. Transparency

a. A covered entity shall, on an annual basis, report to the attorney general aggregate information regarding any warrants for biometric information received during the preceding calendar year by the entity and, if known, by any affiliated data processors and third parties.

b. Covered entities that are required to regularly disclose biometric information as a matter of law shall, on an annual basis, report to the attorney general aggregate information related to such disclosures.

c. The attorney general shall develop standardized reporting forms to comply with this section and make the reports available to the general public online.

Section 5. Enforcement

a. A violation of this chapter or a regulation promulgated under this chapter regarding an individual's biometric information constitutes a rebuttable presumption of harm to that individual.

b. Private right of action. Any individual alleging harm caused by a violation of this chapter may bring a civil action in any court of competent jurisdiction. An individual protected by this chapter shall not be required, as a condition of service or otherwise, to file an administrative complaint with the attorney general or to accept mandatory arbitration of a claim under this chapter. The civil action shall be directed to any covered entity, data processor, or third parties alleged to have committed the violation.

1. In a civil action in which the plaintiff prevails, the court may award

i. liquidated damages of not less than 0.5% of the annual global revenue of the covered entity or $5,000 per violation, whichever is greater, if the defendant conduct was intentional or reckless; or

ii. liquidated damages of not less than 0.1% of the annual global revenue of the covered entity or $1,000 per violation, whichever is greater, if the defendant conduct was negligent;

iii. punitive damages; and

iv. any other relief, including but not limited to an injunction, that the court deems to be appropriate.

v. reasonable attorney's fees and costs, including expert witness fees and other litigation expenses to any prevailing plaintiff.

2. Each instance in which a covered entity, a data processor, or a third party collects, processes, or discloses biometric data with another person in a manner prohibited by this section constitutes a separate violation of this section.

c. Attorney general action. The attorney general may bring an action pursuant to section 4 of chapter 93A against a covered entity, data processor, or third party to remedy violations of this chapter and for other relief that may be appropriate.

d. Non-waivable rights. Any provision of a contract or agreement of any kind, including a covered entity's terms of service or policies, including but not limited to the Biometric Privacy Policy, that purports to waive or limit in any way an individual's rights under this chapter, including but not limited to any right to a remedy or means of enforcement, shall be deemed contrary to state law and shall be void and unenforceable.

e. No private or government action brought pursuant to this chapter shall preclude any other action under this chapter.

Section 6. Non-applicability

a. Nothing in this chapter shall:

1. be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person;

2. be construed to conflict with the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under either Act;

3. be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder;

4. be construed to apply to a contractor, subcontractor, or agent of a government agency or local unit of government when working for that agency or local unit of government, only to the extent of the use of biometric information for such work and so long as it conforms with applicable local and state laws and regulations.

SECTION 2. Biometric Information Collected Before Effective Date

a. Within six months after the Effective Date of this Act, covered entities shall obtain consent in accordance with the provisions of Section 2 of Chapter 93M for any biometric information collected and stored before such Effective Date and shall permanently destroy any biometric information for which they have not obtained consent.

b. The attorney general may adopt regulations, from time to time, in furtherance of the administration of this Act.

SECTION 3. Effective date

a. This Act shall take effect one year after enactment.