HOUSE DOCKET, NO. 3523 FILED ON: 1/17/2025

HOUSE . . . . . No. 96

The Commonwealth of Massachusetts

PRESENTED BY:

David M. Rogers and Andres X. Vargas

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 provide accountability in the use of biometric recognition technology and comprehensive enforcement.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
David M. Rogers	*24th Middlesex*	*1/17/2025*
Andres X. Vargas	*3rd Essex*	*1/17/2025*

HOUSE DOCKET, NO. 3523 FILED ON: 1/17/2025

HOUSE . . . . . No. 96

By Representatives Rogers of Cambridge and Vargas of Haverhill, a petition (accompanied by bill, House, No. 96) of David M. Rogers and Andres X. Vargas relative to the use of biometric recognition technology. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Fourth General Court
(2025-2026)

An Act to provide accountability in the use of biometric recognition technology and comprehensive enforcement.

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. Chapter 110H of the General Laws, as appearing in the 2022 Official Edition, is hereby amended by adding the following chapter:—

Chapter 110I. Regulation of biometric recognition technology

Section 1. Definitions

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

"Agency" , any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or any of its branches, or of any political subdivision thereof.

“Abusive trade practice” , any conduct by a covered entity that 1) materially interferes with the ability of an end user to understand a term or condition of the agreement between covered entities and end users relating to biometric recognition technology or biometric data or 2) takes unreasonable advantage of: a) A lack of understanding on the part of the end user of the material risks, costs, or conditions of the covered entity’s product or service that uses biometric recognition technology; or b) The inability of the end user to protect their interests in selecting or using a covered entity’s product or service; or c) The reasonable reliance by the end user on a covered entity’s representation to act in the interests of the end user.

“Biometric data” means information 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 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 data 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 data 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 data 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 data 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.

“Biometric recognition technology” , Technology that (i) analyzes biometric data; (ii) is used to assign a unique, persistent identifier; or (iii) is used for the unique personal identification of a specific individual.

“Consent” , any freely given, specific, informed and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of biometric data relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use or similar document that contains descriptions of biometric data processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of an abusive trade practice does not constitute consent.

“Controller” , Any covered entity that, alone or jointly with others, determines the purposes and means of processing biometric data.

“Covered entity” , Any person, including corporate affiliates, that collects, stores, or processes biometric data; provided, that the federal government or any state or local government, law enforcement agency, national security agency or intelligence agency shall not be covered entities.

“Data” , Any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

“Deceptive data practice” , Any act or practice involving the processing or transfer of covered data in a manner that constitutes a deceptive act or practice as described in section 2 of chapter 93A.

“Electronic” , Relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

“Encrypted” , Data that has been transformed according to procedures outlined in 45 CFR § 164.312(a)(2)(iv) and (e)(2)(ii) into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation.

“End user” , An individual providing biometric data to a covered entity.

“Harmful data practice” , The processing or transfer of covered data in a manner that causes or is likely to cause: (1) financial, physical, or reputational injury to an individual; (2) physical or other highly offensive intrusion upon the solitude or seclusion of an individual or the individual’s private affairs or concerns, where such intrusion would be highly offensive to a reasonable person; or (3) other substantial injury to an individual.

“Legal effect” , An effect that changes an entity or persons’ legal duties, liabilities, obligations, benefits owed, protections granted by law, or ability to utilize legal remedies.

“Person” , A natural person, corporation, association, partnership or other legal entity.

“Personal information” , For purposes of this section, “personal information” means biometric data.

“Unfair data practice” , The processing or transfer of covered data in a manner that causes or is likely to cause substantial injury to end users which is not reasonably avoidable by end users themselves and not outweighed by countervailing benefits to end users.

Section 2. Duties of loyalty, care, and confidentiality for covered entities

(a) A covered entity shall be prohibited from taking any actions with respect to processing biometric data or designing biometric recognition technologies that conflict with an end user’s best interests.

(b) A covered entity shall be required to secure biometric data from unauthorized access in a reasonable manner that is the same as or more protective than the manner in which the covered entity secures other confidential and sensitive data and shall be prohibited from engaging in harmful data practices.

(c) A covered entity shall not: (i) process or transfer biometric data in any manner not consented to by the end user; (ii) engage in the sale of biometric data to a third party; (iii) disclose biometric data with any other person or entity except as consistent with the duties of loyalty, care, and confidentiality under subsections 2(a), 2(b) and 2(c)(i) and 2(c)(ii),

respectively; or (iv) disclose or share biometric data with any other person unless that person enters into a contract with the covered entity that imposes on the person the same duties of care, loyalty, and confidentiality toward the end user as are imposed on the covered entity under this subsection.

(d) A covered entity shall take reasonable steps to ensure that the practices of any person to whom the online service provider discloses or sells, or with whom the online service provider shares, biometric data fulfill the duties of care, loyalty, and confidentiality assumed by the person under the contract described in subparagraph (c), including by auditing, on a regular basis, the data security and data practices of any such person.

(e) A covered entity shall not discriminate against a consumer because of the withheld consent under this title, including, but not limited to: (i) denying goods or services to the end user; (ii) charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; (iii) providing a different level or quality of goods or services to the end user; (iv) suggesting that the end user will receive a different price or rate for goods or services or a different level or quality of goods or services.

Section 3. Regulating unfair, deceptive, and abusive biometric data practices

(a) A covered entity shall not: (i) engage in a deceptive data practice; (ii) engage in an unfair data practice; or (iii) engage in an abusive trade practice.

(b) It is the intent of the legislature that in construing paragraph (a) of this section in actions unfair and deceptive trade practices, the courts will be guided by the interpretations given by the Federal Trade Commission and the Federal Courts to section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)), as from time to time amended.

(c) The attorney general may make rules and regulations interpreting the provisions of subsection 2(a) of this chapter.

Section 4. Limits on decision-making and public surveillance

(a) Covered entities shall not use biometric data to help make decisions that produce legal effects or similarly significant effects concerning end users. Decisions that include legal effects or similarly significant effects concerning end users include, without limitation, denial or degradation of consequential services or support, such as financial or lending services, housing, insurance, educational enrollment, criminal justice, employment opportunities, health care services, and access to basic necessities, such as food and water.

(b) Covered entities may not operate, install, or commission the operation or installation of equipment incorporating biometric recognition technology in any place, whether licensed or unlicensed, which is open to and accepts or solicits the patronage of the general public.

(c) The legislature finds that the practices covered by this section are matters vitally affecting the public interest for the purpose of applying the Massachusetts Consumer Protection law, chapter 93a. A violation of this section is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the Massachusetts Consumer Protection law, chapter 93a.

Section 5. Applicability of other state and federal laws

This chapter does not relieve a person or agency from the duty to comply with requirements of any applicable general or special law or federal law regarding the protection and privacy of personal information.

Section 6. Enforcement

The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.