Bill Number: H. 96
Title: An Act to provide accountability in the use of biometric recognition technology and comprehensive enforcement
Lead Sponsor: Representative David Rogers
Hearing Date: April 9, 2025
Report Date: June 8, 2025
See Senate Filing: S. 36
Current Law:

- **M.G.L. Chapter 93A** prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce.
- **M.G.L. Chapter 93A § 2** is used, in part, to define "deceptive trade practice" as used in the bill.
- **M.G.L. Chapter 93A § 4** outlines how the Attorney General may bring suit for a violation of Chapter 93A.

Executive Summary: The bill aims to prevent unfair, deceptive or abusive use of Massachusetts residents' biometric information. This extends to information such as fingerprints, retina and iris patterns, voiceprints, DNA sequences, facial characteristics and face geometry, gait, handwriting, keystroke dynamics, and mouse movements.

Legislative History: New File

Section 1. Definitions

"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.

“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.

Applies to any person or business that collects, stores, or processes biometric data, but does not apply to federal, state and local government entities. Defines biometric data as information that pertains to measurable biological or behavioral characteristics of an individual (e.g. fingerprints, retina and iris patterns, voiceprints, D.N.A. sequences, facial characteristics and face geometry, gait, handwriting, keystroke dynamics, and mouse movements).

Section 2. Duties of loyalty, care, and confidentiality for covered entities
Prohibits a covered entity from taking any actions with respect to processing biometric data or designing biometric recognition technologies that conflict with the best interests of the individual who provided the biometric data to the covered entity.
Requires a covered entity obtain the consent of the individual who provided biometric data before processing or transferring said data.

Prohibits the sale of biometric data to any third party.

Requires that a covered entity take reasonable steps to ensure that the practices of any person to whom the online service provider discloses biometric data fulfill the same duties of care, loyalty, and confidentiality and requires auditing, on a regular basis, the data security and data practices of any such person.

Prohibits discrimination against a consumer because they withheld consent, including discrimination against a consumer by denying goods or services, charging different prices or rates, providing a different level or quality of goods or services, 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
Prohibits a covered entity from engaging in any deceptive, unfair, or abuse data practice. Grants the Attorney General rulemaking authority.

Section 4. Limits on decision-making and public surveillance
Prevents covered entities from using biometric data to help make decisions that produce legal effects or similarly significant effects concerning end users, which include 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. Prohibits a covered entity from operating, installing, or commissioning the operation or installation of equipment incorporating biometric recognition technology in any place which is open to and accepts or solicits the patronage of the general public.

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
Grants the Attorney General regulatory and enforcement authority under section 4 of Chapter 93A.