Joint Committee on Advanced Information Technology, the Internet and Cybersecurity 2025-2026 (194th) Bill Summary

---

Bill Number: H. 97
Title: An Act protecting consumers in interactions with artificial intelligence systems
Lead Sponsor: Representative David M. Rogers, Andres X. Vargas
Hearing Date: September 11, 2025
Report Date: November 10, 2025
Current Law:
M.G.L. c. 66 § 10 governs the response to requests for public records.
Title XV of Part I of the Massachusetts General Laws allows for the regulation of trade.
M.G.L. c. 93 § 42 defines "trade secret" as used in §§ 42-42G.
M.G.L. c. 93A prohibits unfair and deceptive trade practices in the commonwealth.
M.G.L. c. 156D applies to business corporations in the commonwealth.
M.G.L. c. 167 defines "bank," "credit union," and "out-of-state bank" for the purpose of regulating banks in the commonwealth.
M.G.L. c. 175 defines "insurer" for the purpose of regulating insurance in the commonwealth.
M.G.L. c. 176 defines "fraternal benefit society" for the purpose of regulating fraternal benefit societies in the commonwealth.

Executive Summary: Requires AI developers to provide detailed documentation about their systems' risks and limitations, while deployers must implement risk management programs and conduct regular impact assessments. Companies using high-risk AI for consequential decisions (employment, housing, healthcare, etc.) must notify consumers and provide explanations for adverse decisions, along with appeal opportunities. The Massachusetts Attorney General receives exclusive enforcement authority and can promulgate additional rules, with violations treated as unfair trade practices under 93A.

Legislative History: New File

Summary:
Defines "Algorithmic discrimination" as any condition in which the use of an artificial intelligence system results in an unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, veteran status, or other classification protected under the laws of this state or federal law.

Defines "High-risk artificial intelligence system" as any artificial intelligence system that, when deployed, makes, or is a substantial factor in making, a consequential decision. Certain technologies such as anti-fraud technology that does not use facial recognition technology, anti-malware, anti-virus, spell-check, and others are not included in the definition unless the technologies, when deployed, make, or are a substantial factor in making, a consequential decision.

Defines "Consequential decision" as a decision that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of:

- education enrollment or an education opportunity;
- employment or an employment opportunity;
- a financial or lending service;
- an essential government service;
- health-care services;
- housing;
- insurance; or
- a legal service.

Defines "Deployer" as a person doing business in this state that deploys a high-risk artificial intelligence system.

Defines "Developer" as a person doing business in this state that develops or intentionally and substantially modifies an artificial intelligence system.

Section 2: Developer Requirements

Developers must:

- Use reasonable care to prevent algorithmic discrimination within 6 months of the law's effective date
- Provide extensive documentation to deployers including:
    - Training data summaries
    - Known limitations and discrimination risks
    - Evaluation methods and mitigation measures
    - Proper usage guidelines
- Publish public statements about their high-risk AI systems and discrimination management
- Report discovered discrimination incidents to the Attorney General and deployers within 90 days
- Comply with disclosure requests from the Attorney General

Trade secrets, as defined in section 42 (4) of chapter 93 of the General Laws, as appearing in the 2022 Official Edition and security-sensitive information are protected from disclosure requirements.

Section 3: Deployer Requirements

Deployers must use reasonable care to prevent algorithmic discrimination and must implement risk management policies following recognized frameworks

The risk management policy and program must be an iterative process planned, implemented, and regularly and systematically reviewed and updated over the life cycle of a high-risk artificial intelligence system, requiring regular, systematic review and updates. A risk management policy and program implemented and maintained pursuant to this subsection must be reasonable considering:

- The guidance and standards set forth in the latest version of the "Artificial Intelligence Risk Management Framework" published by the National Institute of Standards and Technology in the United States Department of Commerce, standard ISO/IEC 42001 of the International Organization for Standardization, or another nationally or internationally recognized risk management framework for artificial intelligence systems, if the standards are substantially equivalent to or more stringent than the requirements of this chapter; or
- Any risk management framework for artificial intelligence systems that the Attorney General, in the Attorney General's discretion, may designate;
- The size and complexity of the deployer;
- The nature and scope of the high-risk artificial intelligence systems deployed by the deployer, including the intended uses of the high-risk artificial intelligence systems; and
- The sensitivity and volume of data processed in connection with the high-risk artificial intelligence systems deployed by the deployer.

Not later than 6 months after the effective date of this act, a deployer, or a third party contracted by the deployer, shall complete an impact assessment for a deployed high-risk artificial intelligence system at least annually and within ninety days after any intentional and substantial modification to the high-risk artificial intelligence system is made available.

An impact assessment completed pursuant to this subsection must include, at a minimum, and to the extent reasonably known by or available to the deployer:

- A statement by the deployer disclosing the purpose, intended use cases, and deployment context of, and benefits afforded by, the high-risk artificial intelligence system;

- An analysis of whether the deployment of the high-risk artificial intelligence system poses any known or reasonably foreseeable risks of algorithmic discrimination and, if so, the nature of the algorithmic discrimination and the steps that have been taken to mitigate the risks;
- A description of the categories of data the high-risk artificial intelligence system processes as inputs and the outputs the high-risk artificial intelligence system produces;
- If the deployer used data to customize the high-risk artificial intelligence system, an overview of the categories of data the deployer used to customize the high-risk artificial intelligence system;
- Any metrics used to evaluate the performance and known limitations of the high-risk artificial intelligence system;
- A description of any transparency measures taken concerning the high-risk artificial intelligence system, including any measures taken to disclose to a consumer that the high-risk artificial intelligence system is in use when the high-risk artificial intelligence system is in use; and
- A description of the post-deployment monitoring and user safeguards provided concerning the high-risk artificial intelligence system, including the oversight, use, and learning process established by the deployer to address issues arising from the deployment of the high-risk artificial intelligence system.

An impact assessment completed pursuant to this subsection following an intentional and substantial modification to a high-risk artificial intelligence system not later than 6 months after the effective date of this act, must include a statement disclosing the extent to which the high-risk artificial intelligence system was used in a manner that was consistent with, or varied from, the developer's intended uses of the high-risk artificial intelligence system.

Deployers also must conduct impact assessments annually and after substantial modifications, including:

    - Purpose and intended uses
    - Discrimination risk analysis
    - Data categories processed
    - Performance metrics and limitations
    - Transparency measures
    - Post-deployment monitoring

Before the deployment and use of tech that may make consequential decisions, deployers must notify consumers that AI is being used, explain the system's purpose, provide contact information, and inform consumers of any opt-out rights for data profiling. All consumer notices must be provided directly in plain language, in all languages the deployer normally uses for business communications, and in formats accessible to people with disabilities.

When AI contributes to unfavorable outcomes, deployers must disclose the principal reasons, explain how the AI contributed, identify what data was processed and its sources, and provide opportunities for data correction and appeals with human review.

Companies with fewer than 50 employees using unmodified third-party AI systems have reduced compliance requirements, but must still share developer impact assessments with consumers.

Section 4: General AI Disclosure

Any AI system intended to interact with consumers must disclose its artificial nature, unless it would be obvious to a reasonable person.

Section 5: Compliance Exceptions

Exemptions are granted under various conditions, including for:

- Federally regulated systems (FDA-approved medical devices, etc.)
- Federal contract work (except employment/housing decisions)
- HIPAA-covered healthcare recommendations
- Banks and insurers subject to equivalent federal oversight
- Activities protected by First Amendment rights

Section 6: Enforcement

The Attorney General has exclusive enforcement authority. Violations constitute unfair trade practices under Chapter 93A. The Attorney General authority to create detailed implementing regulations for all aspects of the law including:

(1) the documentation and requirements for developers pursuant to section 2 (b);
(2) the contents of and requirements for the notices and disclosures required by sections 2 (c) and (g); 3 (d), (e), (g), and (i); and 4;
(3) the content and requirements of the risk management policy and program required by section 3 (b);
(4) the content and requirements of the impact assessments required by section 3 (c);

(5) the requirements for the rebuttable presumptions set forth in sections 2 and 3; and

(6) the requirements for the affirmative defense set forth in section 6 (c), including the process by which the attorney general will recognize any other nationally or internationally recognized risk management framework for artificial intelligence systems.

This Chapter does not create a private right of action for consumers.