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

Bill Number: H. 4746
Title: An Act establishing the Massachusetts consumer data privacy act
Lead Sponsor: Representative Tricia Farley-Bouvier
Current MA Law:
● **M.G.L. Chapter 12 § 11** establishes annual enforcement reporting procedures for the attorney general's office.
● **M.G.L. Chapter 12 § 11I½** provides protections for reproductive and gender affirming healthcare in the Commonwealth.
● **M.G.L. Chapter 76 § 1** defines "private school" as used in the bill.
● **M.G.L. Chapter 93 § 42** defines "trade secret" as used in the bill.
● **M.G.L. Chapter 93 § 115** protects information regarding legally protected health care under section 11I ½ from subpoena and other court orders without meeting certain requirements.
● **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 93H** regulates cybersecurity and establishes notification for certain data breaches.
● **M.G.L. Chapter 110A** defines "agent, broker-dealer, investment adviser or investment adviser" for the purposes of securities regulation.
● **M.G.L. Chapter 151B** prohibits employment discrimination based on status as a member of a protected class.

Executive Summary: Inserts the Massachusetts Consumer Data Privacy Act (MCDPA) as a new chapter of the Massachusetts General Laws. The MCDPA requires data minimization. Data holders ("controllers") must limit the collection, processing, or transfer of consumer's personal data to what is adequate, relevant, and reasonably necessary to provide their services. Data minimization includes deleting or removing information when it is no longer necessary in order to mitigate the misuse of personal information and the risks associated with data breaches. The bill requires additional protections for a consumer's sensitive data – health information, financial information, specific geolocation information, etc. Mandates clear, affirmative, informed consent (opt-in) for sensitive data transfers or sales. Includes a ban on processing the data of minors for targeted advertising. The bill also requires data protection assessments for high-risk processing activities, with reports submitted to the Attorney General and summaries of such assessments made accessible to the public. The MCDPA includes Attorney General enforcement, a private right of action, and rulemaking authority for the enforcement of the law.

Section 1. Definitions

Includes specifications for targeted advertising. “Targeted advertising” means displaying to an individual or device identified by a unique persistent identifier an online advertisement that is selected based on known or predicted preferences, characteristics, behavior, or interests associated with that individual or device. It does not include first-party advertising or contextual advertising.

“Contextual advertising” means displaying an advertisement that does not vary based on the identity of the individual recipient and is based on the immediate content of a webpage on which the advertisement appears (e.g. advertising for sporting goods stores in the sports section of a news website), a specific request of a consumer for information or feedback, or a consumer’s immediate presence in a geographic area with a radius no smaller than 10 miles or an area reasonably estimated to include online activity from at least 5,000 users, but not including precise geolocation data.

“First-party advertising” means processing by a first party of its own data for the purposes of advertising that is carried out through direct communications with a consumer, in a physical location operated by the first party, or through display of an ad on the first party’s own website, app, or other online content. A “first party” is defined as a consumer-facing controller with which the consumer intends or expects to interact.

“Consumer” means an individual who is a resident of this state. “Consumer” does not include an individual acting as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

“Consumer health and wellness data” means personal data that is collected by a health and wellness device or application that is not otherwise biometric data, neural data, or personal data that reveals a mental or physical health condition, diagnosis, disability, or treat

“Controller” means a person who, alone or jointly with others, determines the purpose and means of collecting or processing personal data.

“First-party data” means personal data collected directly from a consumer by a first party, including based on a visit by the consumer to or use by the consumer of a website, a physical location, or an online service operated by the first party.

“Gender-affirming health care services” means all medical care relating to the treatment of gender dysphoria as set forth in the most recent edition of the American Psychiatric Association's “Diagnostic and Statistical Manual of Mental Disorders” and gender incongruence, as defined in the most recent revision of the “International Statistical Classification of Diseases and Related Health Problems.”

“Gender-affirming health data” means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, gender-affirming health care services.
“Minor” means any consumer who is younger than 18 years of age.

“Precise geolocation data” means information derived from technology, including, but not limited to, latitude and longitude coordinates from global positioning system mechanisms or other similar positional data, that reveals the past or present physical location of an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals with precision and accuracy within a radius of one thousand seven hundred fifty feet.

“Precise geolocation data” does not include the content of communications, a photograph or video, metadata associated with a photograph or video that cannot be linked to an individual, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

“Reproductive or sexual health care” means any health care-related services or products rendered or provided concerning a consumer's reproductive system or sexual well-being, including, but not limited to, any such service or product rendered or provided concerning

(A) an individual health condition, status, disease, diagnosis, diagnostic test or treatment,
(B) a social, psychological, behavioral or medical intervention,
(C) a surgery or procedure, including, but not limited to, an abortion,
(D) a use or purchase of a medication, including, but not limited to, a medication used or purchased for the purposes of an abortion,
(E) a bodily function, vital sign or symptom,
(F) a measurement of a bodily function, vital sign or symptom, or
(G) an abortion, including, but not limited to, medical or nonmedical services, products, diagnostics, counseling or follow-up services for an abortion.

“Reproductive or sexual health data” means any personal data concerning an effort made by a consumer to seek, or a consumer's receipt of, reproductive or sexual health care.

“Sensitive data” means personal data that includes:
(i) data revealing a consumer’s:
(A) racial or ethnic origin, color, national origin or citizenship or immigration status;
(B) religious beliefs;
(C) mental or physical health condition, or diagnosis, disability or treatment, including, but not limited to, gender-affirming health data, reproductive or sexual health data or legally-protected health care data;
(D) sex life, sexual orientation, status as transgender or non-binary;
(E) union membership;

(F) status as a victim of a crime; or
(G) status as a military servicemember or veteran;
(ii) consumer health and wellness data;
(iii) genetic, neural, or biometric data;
(iv) personal data of a consumer that a controller knows, or willfully disregards, is a minor;
(v) precise geolocation data;
(vi) a government-issued identifier, including a Social Security number, passport number or driver's license number, that is not required by law to be displayed in public;
(vii) account names, passwords, usernames, access codes, security questions or answers, or other credentials and information used to log in to an account or device.

Section 2. Applicability

Applies to businesses operating in Massachusetts or targeting Massachusetts residents that (a) collect/process data from at least 100,000 consumers (not counting certain transaction information needed to complete sales) (b) derived gross revenue from selling personal data, or (c) collected or processed sensitive data. The payment transaction exemption allows businesses to process data solely for completing payments if deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a business's return policy.

Section 3. Scope

Outlines specific exemptions to the law, including government entities and certain types of protected health information. Exempts various categories of data already regulated by federal laws like HIPAA, Gramm-Leach-Bliley Act, and Family Educational Rights and Privacy Act. The section also clarifies that compliance with COPPA's parental consent requirements satisfies this law's parental consent obligations.

Exemptions do not apply for the ban on the sale of precise geolocation data provided for in paragraph (4) of subsection (a) of Section 6.

Section 4. Consumer Rights (Data Subject Rights)

Consumers are granted several rights over their data, including the right to confirm data collection, access their data, correct inaccuracies, delete their data, and opt out of targeted advertising. Controllers must respond to consumer requests within 45 days. The section includes specific provisions for authenticating requests and handling appeals. Information provided in response to a consumer request shall be provided by a controller, free of charge, no less than two times during any twelve-month period.

- Right to Access

    - ○ Individuals have the right to confirm whether or not a controller is collecting or processing personal data,including but not limited to, any inferences about the consumer derived from such personal information. If the covered entity transfers this data to any third parties, the consumer is also able to request a list of third parties that the controller has transferred data to.
- Right to Correct
    - ○ Individuals may request to correct any inaccurate information that is processed by the covered entity.
    - ○ Individuals may instruct the covered entity to notify all third parties or service providers to which the covered entity has transferred this covered data about the corrected information.
- Right to Delete
    - ○ Individuals may request to delete personal data that is provided by, or obtained about, the consumer, including personal data the consumer provided to the controller, data the controller obtained from another source, and any derived data.
    - ○ Individuals may instruct the covered entity to notify all third parties of the individual's deletion request.
- Right to Transfer
    - ○ Individuals may request an export copy of their personal data collected or processed by the controller in a portable and readily usable format that allows the consumer to transmit the data elsewhere.
- Right to Opt Out
    - ○ Individuals have the right to opt out of the collection and processing of personal data for the purposes of targeted advertising or for the profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer.
    - ○ Individuals have the right to opt out of the sale of personal data.

Section 5. Authorized Agent

Allows consumers to designate authorized agents to exercise their rights under the law on their behalf. Controllers must verify both the identity of the consumer and the authority of the agent.

Section 6. Actions of Controllers

Controllers must limit data collection to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer, including any routine administrative, operational, or account-servicing activity.

What is "requested by the consumer" shall be based on objective circumstances that indicate that a consumer is seeking the product or service. This includes factors like the relationship

between the consumer and controller, the type of and amount of data the controller seeks to collect, the source and method for collecting, and the degree to which the involvement of processors and third parties in the collecting or processing of personal data. Controllers shall also not process or transfer personal data in a manner that is inconsistent with the reasonable expectations of the consumer.

Controllers shall not collect, process, or transfer sensitive data except when such collection, processing, or transfer is strictly necessary to provide a specific product or service requested by the consumer. Controllers shall establish, implement and maintain reasonable administrative, technical, and physical data security practices to protect personal data in a manner appropriate to the volume and nature of personal data. This includes disposing of personal data in accordance with a retention schedule that requires the deletion of personal data when it is no longer necessary for the purpose for which the data was collected, processed, or transferred or when required by law. Controllers cannot sell a consumer's sensitive data without affirmative consent.

Controllers cannot sell precise geolocation data.

Controllers cannot process or sell a consumer’s data for the purpose of targeted or first party advertising if they know that consumer is a minor.

Controllers must provide clear privacy notices and cannot discriminate against consumers who exercise their rights. The section requires controllers to offer easy-to-use opt-out and affirmative consent mechanisms. Controllers cannot not discriminate or retaliate against a consumer for exercising any of the consumer rights contained in this chapter, or for refusing to agree to the collection or processing of personal data for a separate product or service, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer.

Subsection (b) of Section 6 allows for the processing and transfer of personal data of a consumer who participates in a loyalty or rewards program provided that such transfer is clearly and conspicuously disclosed in the terms of the program and that the sale of personal data shall not be a condition of participation in the program.

Controllers must provide consumers with a reasonably accessible, clear and meaningful privacy notice that includes:

- Categories of personal data collected (including a separate list of categories of sensitive data)
- Purpose for collecting each category of data
- How consumers can exercise their rights
- Categories of personal data transferred to third parties
- Categories of third parties receiving personal data
- Data retention timeframes or criteria for determining retention
- Contact method for consumers (email address)

If any material changes are made to such privacy notices, controllers must notify affected consumers before implementing changes and allow consumers the opportunity to withdraw or renew consent.

Controllers must establish at least two secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this chapter, including an opt out mechanism to opt out of targeted advertising, the sale of data, and profiling for automated decisions.

Section 7. Responsibilities of Processors and Controllers

Establishes the relationship and obligations between processors and controllers through mandatory contractual provisions, including that the contract shall also require that the processor ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data, and at the controller’s direction, delete or return all personal data to the controller. Processors must follow controllers' instructions and help them comply with the law's requirements. Includes specific security requirements and clarifies when a processor might be considered a controller.

Section 8. Data Protection Assessments

Controllers must conduct and document data protection assessments for high-risk processing activities, including practices like targeted advertising, the sale of personal data, and processing sensitive data. Data protection assessments conducted shall identify the categories of personal data collected, the purposes for collecting such personal data, whether personal data is being transferred. These assessments must be submitted to the Attorney General within 30 days and be publicly available. Data protection assessments must be conducted before controllers may initiate processing that presents a heightened risk. The section requires regular reviews and updates of these assessments throughout the processing activity's lifecycle.

The bill defines processing that presents a heightened risk of harm to a consumer as: “the collection or processing of personal data for the purposes of targeted advertising; the sale of personal data; the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of: unfair or deceptive treatment of, or unlawful disparate impact on, consumers, financial, physical or reputational injury to consumers, a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or other substantial injury to consumers; the collection or processing of sensitive data; and processing data on services predominantly used by minors.”

Section 9. De-identified Data

Controllers must take technical measures to ensure de-identified data cannot be re-associated with individuals and publicly commit to maintaining it in de-identified form. Requires contractual obligations for recipients of de-identified data to comply with provisions of this act and requires controllers to exercise oversight over recipients of de-identified data and take appropriate steps to address any breaches of those contractual commitments.

The section includes oversight requirements for controllers transferring de-identified data.

Section 10. Limitations

This section outlines various exemptions allowing controllers to process data for specific purposes like law enforcement, research, and security. It protects privileged communications and First Amendment rights. The section requires that any exempt processing must be reasonable, necessary, and proportionate to the stated purpose. Outlines that nothing in this chapter shall be construed to restrict a controller's or processor's ability to provide, maintain, improve, or update a product or service specifically requested by the consumer.

Section 11. Rulemaking

The Attorney General is authorized to promulgate rules and regulations to implement the Act, including but not limited to establishing baseline technical requirements to determine if a given dataset has been sufficiently de-identified, establish reasonable data security practices, establish a nonexclusive list of practices that constitute dark patterns or otherwise violate the requirements of this chapter regarding a consumer's affirmative consent, and establish a nonexclusive list of data collection, processing, and transfer practices that constitute unfair or deceptive practices in trade or commerce.

Section 12. Enforcement

A violation of this chapter constitutes an injury to that individual and shall be deemed an unfair or deceptive act or practice in the conduct of trade or commerce under the Massachusetts Consumer Protection Law (MGL Ch. 93A).

Notwithstanding sections 9 and 11 of said chapter 93A, the attorney general shall have exclusive authority to bring a civil action against any controller or processor other than a controller or processor that is a large data holder that violates this chapter or a regulation adopted under this chapter to:

> (1) enjoin an act or practice that is in violation of this chapter or a regulation adopted under this chapter, including an order that an entity retrieve any personal data transferred in such violation;

(2) enforce compliance with this chapter or a regulation adopted under this chapter, including seeking declaratory relief;

(3) obtain damages, including punitive damages, restitution of any money or property obtained directly or indirectly by any such violation, and disgorgement of any profits, assets, property, or data obtained directly or indirectly by any such violation on behalf of the residents of the commonwealth;

(4) impose civil penalties in an amount not more than $5,000 per violation;

(5) obtain investigative costs, reasonable attorney's fees and other litigation costs, including, but not limited to, expert fees, reasonably incurred; and

(6) obtain any such other and further relief as the court may deem proper.

The Attorney General can also bring civil actions with penalties. If the court finds that a defendant has engaged in flagrant, willful, and repeated violations of this chapter in an action brought by the Attorney General, the court may issue an order to suspend or prohibit the defendant from operating in the commonwealth in addition to any other remedies under this section. The section prohibits contractual waivers of consumer rights.

The Attorney General shall create, maintain and monitor a mechanism for consumers to report potential violations of this chapter and issue reports on the enforcement of the chapter to the clerks of the House and Senate, the Speaker of the House, the Senate President, and both chairs of the advanced information technology, the internet and cybersecurity committee.

Section 13. Relationship to Other Laws

Clarifies that this act does not limit the rights or responsibilities established by other privacy laws in Massachusetts.

Section 14. Location Information of Non-Residents

Requires that specific geolocation information of visitors to the Commonwealth is treated the same way as resident's location information.

Section 15. Mergers, Acquisitions, and Bankruptcy

A controller may transfer personal data to a third party in the context of a merger, acquisition, bankruptcy or similar transaction when the third party assumes control, in whole or in part, of the controller's assets, only if the controller, in a *reasonable time* prior to the transfer, provides an affected consumer with notice describing the transfer, including the name of the entity receiving the consumer's personal data and the applicable privacy policies of such entity; and a reasonable opportunity to withdraw previously provided consent related to the consumer's personal data.

In any transaction involving the transfer of genetic, neural, or biometric data, the reasonable opportunity shall be no shorter than 60 days.

Section 16. Browser Privacy Settings

By January 1, 2027, a person shall not develop or maintain a browser that does not include a setting that enables a consumer to send an opt-out preference signal, as described in section 6(e)(2), to controllers or processors that the consumer interacts with through the browser.

Effective Dates

The Massachusetts Consumer Data Privacy Act takes effect 180 days after enactment. The first data protection assessments required by section 8 of the Massachusetts Consumer Data Privacy Act shall be completed no later than the first anniversary of the effective date of the Act.