SENATE . . . . . No. 2516

The Commonwealth of Massachusetts

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

SENATE, May 12, 2025.

The committee on Advanced Information Technology, the Internet and Cybersecurity to whom was referred the petition (accompanied by bill, Senate, No. 45) of Michael O. Moore, Joanne M. Comerford, Rebecca L. Rausch, James B. Eldridge and others for legislation to establish the Massachusetts Data Privacy Protection Act, report the accompanying bill (Senate, No.).

For the committee,
Michael O. Moore

FILED ON: 5/9/2025

SENATE . . . . . No. 2516

The Commonwealth of Massachusetts

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

An Act establishing the Massachusetts data privacy act.

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 2022 Official Edition, are hereby amended by inserting after chapter 93L the following chapter:

Chapter 93M. Massachusetts Data Privacy Act

Section 1. Definitions.

(a) As used in this chapter, unless the context otherwise requires:

(1) "Affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by, or is under common control with another legal entity. For the purposes of this subdivision, "control" and "controlled" mean:

(A) ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of a company;

(B) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(C) the power to exercise controlling influence over the management of a company.

(2) “Affirmative Consent” means a clear affirmative act signifying a consumer's freely given, specific, informed, revokable, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a controller, provided that:

(A) the request is provided to the consumer in a clear and conspicuous stand-alone disclosure;

(B) the request includes a description of the processing purpose for which the consumer’s consent is sought and:

(1) clearly distinguishes between an act or practice that is necessary to fulfill a request of the consumer and an act or practice that is for another purpose;

(2) clearly states the specific categories of personal data that the controller intends to collect, process, or transfer under each act or practice; and

(3) is written in easy-to-understand language and includes a prominent heading that would enable a reasonable consumer to identify and understand each act or practice;

(C) the request clearly explains the consumer's rights related to consent;

(D) the request is made in a manner reasonably accessible to and usable by consumers with disabilities;

(E) the request is made prior to the controller’s implementation of the act or practice;

(F) the request is made available to the consumer in each language in which the controller provides a product or service for which authorization is sought;

(G) the option to refuse to give consent is at least as prominent as the option to give consent and the option to refuse to give consent takes the same number of steps or fewer as the option to give consent; and

(H) affirmative consent to an act or practice is not inferred from the inaction of the consumer or the consumer's continued use of a service or product provided by the controller.

"Affirmative Consent" does not include:

(A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;

(B) hovering over, muting, pausing, or closing a given piece of content;

(C) agreement obtained through the use of a false, fictitious, fraudulent, or materially misleading statement or representation; or

(D) agreement obtained through the use of dark patterns or deceptive design.

(3) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under this chapter is being made by, or on behalf of, the consumer who is entitled to exercise such consumer rights with respect to the personal data at issue.

(4) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint or vocal biomarker, eye retinas, irises, gait or personally identifying physical movement or patterns, or other unique biological patterns or characteristics that can be used to identify a specific individual.

"Biometric data" does not include:

(A) a digital or physical photograph,

(B) an audio or video recording, or

(C) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

(5) “Business associate” has the same meaning as provided in HIPAA.

(6) “Child” has the same meaning as provided in COPPA.

(7) “Closed-Loop Referral System” or “CLRS” means any system that: (1) stores the social care information of one or more individuals; (2) enables the sharing of social care information with and between participating entities for the purpose of referring individuals for social care; and (3) is capable of updating or showing updated referral activity, including data related to participating organizations completing referrals.

(8) “Collect” means buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring personal data by any means.

(9) “Consumer” means an individual who is a resident of Massachusetts or is present in Massachusetts, including those identified by a unique persistent identifier.

(10) "Contextual advertising” means displaying or presenting an advertisement that does not vary based on the identity of the individual recipient and is based solely on:

(A) the immediate content of a webpage or online service within which the advertisement appears; or

(B) a specific request of the consumer for information or feedback if displayed in proximity to the results of such request for information;

Provided, however, that a controller may use the following types of personal data to display a contextual advertisement so long as the personal data is not used to make inferences about the consumer, profile the consumer, or for any other purpose, and that the consumer may use technical means to obfuscate or change their physical location and to specify a language preference:

(A) such technical specifications as are necessary for the ad to be delivered and display properly on a given device;

(B) 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; or

(C) the consumer's language preferences, as inferred from context, browser settings, or user settings.

(11) "Controller" means a person who, alone or jointly with others, determines the purpose and means of collecting or processing personal data.

(12) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to said act, as said act and such regulations, rules, guidance and exemptions may be amended from time to time.

(13) "Covered entity" has the same meaning as provided in HIPAA.

(14) “Dark pattern or deceptive design” means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice, and includes, but is not limited to, any practice the Federal Trade Commission refers to as a “dark pattern”.

(15) “Data broker” means a controller, or a unit or units of a controller, separately or together, that knowingly: (a) processes and sells the personal data of a consumer with whom the controller does not have a direct relationship; or (b) licenses to third parties the personal data of a consumer with whom the controller does not have a direct relationship. For the purposes of this definition, direct relationship with a controller means a consumer is a: (a) customer, client, subscriber, user, or registered user of the controller's goods or services within the last five calendar years; (b) employee, contractor, or agent of the controller; or (c) investor in the controller.

(16) “Decisions that produce legal or similarly significant effects concerning the consumer” means decisions that result in access to, or the provision or denial by the controller of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services.

(17) “De-identified data” means data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data:

(A) takes reasonable physical, administrative, and technical measures to ensure that such data cannot be associated with an individual or be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual,

(B) publicly commits to process such data only in a de-identified fashion and not attempt to re-identify such data, and

(C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

(18) "Derived data" means personal data that is created by the derivation of information, data, assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or another source of information or data about an individual or an individual's device.

(19) "Device" means any electronic equipment capable of collecting, processing, or transferring data that is used by one or more individuals or households.

(20) "Genetic information", any data, regardless of its format, that concerns an individual's genetic characteristics, including but not limited to:

(i) raw sequence data that results from the sequencing of the complete, or a portion of the, extracted deoxyribonucleic acid (DNA) of an individual; or

(ii) genotypic and phenotypic information that results from analyzing raw sequence data described in subparagraph (i).

(21) "First party" means a consumer-facing controller with which the consumer intends or expects to interact.

(22) "First-party advertising" means processing by a first party of its own first-party data for the purposes of advertising and marketing and carried out:

(A) through direct communications with a consumer, such as direct mail, email, or text message communications;

(B) in a physical location operated by the first party; or

(C) through display or presentation of an advertisement on the first party's own website, application or its other online content.

"First-party advertising" includes marketing measurement related to such advertising and marketing.

(23) "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.

(24) "Gender-affirming health care services" means all supplies, care and services of a medical, behavioral health, mental health, surgical, psychiatric, therapeutic, diagnostic, preventative, rehabilitative or supportive nature relating to the treatment of gender dysphoria.

(25) "Gender-affirming health data" means any personal data concerning a past, present, or future effort made by a consumer to seek, or a consumer's receipt of, gender-affirming health care services.

(26) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq., as amended from time to time.

(27) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly, including but not limited to, by reference to an identifier such as

a name, an identification number, specific geolocation data or historical pattern of geolocation data, or an online identifier.

"Large data holder" means a controller or processor that in the most recent calendar year:

(i) had annual gross revenues of $200,000,000 or more; and

(ii) collected, processed, or transferred the personal data of more than 2,000,000 individuals or devices that identify or are linked or reasonably linkable to one or more individuals, excluding personal data collected and processed solely for the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested product or service; or the sensitive data of more than 200,000 individuals or devices that identify or are linked or reasonably linkable to one or more individuals.

The term "large data holder" does not include any instance in which the controller or processor would qualify as a large data holder solely on the basis of collecting or processing personal email addresses, personal telephone numbers, or log-in information of an individual or device to allow the individual or device to log in to an account administered by the controller or service provider.

(28) "Legally-protected health care activity", means (i) the exercise and enjoyment, or attempted exercise and enjoyment, by any person of rights to reproductive or sexual health care or gender-affirming health care services secured by the constitution or laws of the commonwealth or the provision of insurance coverage for such services; or (ii) any act or omission undertaken to aid or encourage, or attempt to aid or encourage, any person in the exercise and enjoyment, or attempted exercise and enjoyment, of rights to reproductive or sexual health care or gender-affirming health care services secured by the constitution or laws of the

commonwealth or to provide insurance coverage for such services; provided, however, that the provision of such a health care service by a person duly licensed under the laws of the commonwealth and physically present in the commonwealth and the provision of insurance coverage for such services shall be legally protected if the service is permitted under the laws of the commonwealth, regardless of the patient's location; and provided further, that "legally-protected health care activity" shall not include any service rendered below an applicable professional standard of care or that would violate anti-discrimination laws of the commonwealth.

(29) "Legally-protected health care data" means any personal data concerning past, present, or future legally-protected health care activity.

(30) "Marketing measurement" means measuring and reporting on marketing performance or media performance by the controller, including processing personal data for measurement and reporting of frequency, attribution, and performance.

(31) "Material" means, with respect to an act, practice, or representation of a controller, including a representation made by the controller in a privacy notice or similar disclosure to individuals, involving the collection, processing, or transfer of personal data, that such act, practice, or representation is likely to affect a reasonable individual's decision or conduct regarding a product or service.

(32) "Minor" means any consumer who is younger than 18 years of age.

(33) "Neural data" means any information that is generated by measuring the activity of an individual's central or peripheral nervous system.

(34) “OCABR” means the Office of Consumer Affairs and Business Regulation.

(35) “Participating organization” means any entity that has the ability to create, receive, or update referrals, or other social care information in a CLRS, including, but not limited to, healthcare providers, health plans, public agencies, charitable and nonprofit organizations, CLRS technology vendors, and entities that provide social care.

(36) “Person” means an individual, association, company, limited liability company, corporation, partnership, sole proprietorship, trust or other legal entity.

(37) “Personal data” means any information, including derived data and unique persistent identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or a device that identifies or is linked or reasonably linkable to an individual. “Personal data” does not include de-identified data or publicly available information.

(38) “Precise geolocation data” means information derived from technology or a device, 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 one or more individuals with precision and accuracy within a radius of one thousand seven hundred fifty feet or less.

“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.

(39) “Process” and “processing” mean any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the use, storage, disclosure, analysis, deletion or modification of personal data.

(40) “Processor” means a person who collects, processes, or transfers personal data on behalf of, and at the direction of, a controller or another processor, or a Federal, State, Tribal, or local government entity.

(41) “Profiling” means any form of processing performed on personal data to evaluate, analyze or predict personal aspects including an individual’s economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(42) “Protected health information” has the same meaning as provided in HIPAA.

(43) “Publicly available information” means information that has been lawfully made available to the general public from:

(A) federal, state or municipal government records, if the person collects, processes, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity;

(B) widely distributed media; or

(C) a disclosure to the general public as required by federal, state, or local law.

“Publicly available information” does not include:

(A) Any obscene visual depiction, as defined in section 1460 of title 18, United States Code;

(B) any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive data with respect to a consumer;

(C) biometric data;

(D) personal data that is created through the combination of personal data with publicly available information;

(E) genetic information, unless otherwise made publicly available by the individual to whom the information pertains;

(F) information made available by a consumer on a website or online service made available to all members of the public, for free or for a fee, where the consumer has restricted the information to a specific audience; or

(G) intimate images, authentic or computer-generated, known to be nonconsensual.

(44) "Reproductive or sexual health care" means all supplies, care and services of a medical, behavioral health, mental health, surgical, psychiatric, therapeutic, diagnostic, preventative, rehabilitative or supportive nature relating to pregnancy, contraception, assisted reproduction, miscarriage management, the termination of a pregnancy. a consumer's reproductive system or sexual well-being, including, but not limited to, any such supplies, care and services 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.

(45) “Reproductive or sexual health data” means any personal data concerning a past, present, or future effort made by a consumer to seek, or a consumer's receipt of, reproductive or sexual health care.

(46) “Sale of personal data” means the exchange of personal data for monetary or other valuable consideration by the controller to a third party.

“Sale of personal data” does not include:

(A) the disclosure of personal data to a processor that processes the personal data on behalf of the controller if limited to the purposes of the processing;

(B) the disclosure of personal data to a third party for purposes of providing a product or service affirmatively requested by the consumer;

(C) the disclosure or transfer of personal data to an affiliate of the controller;

(D) with the consumer’s affirmative consent, the disclosure of personal data where the consumer affirmatively directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party; or

(E) the disclosure of personal data that the consumer:

(i) intentionally made available to the general public via a channel of mass media; and

(ii) did not restrict to a specific audience.

(47) "Sensitive data" means personal data that includes:

(A) A government-issued identifier, such as a Social Security number, passport number, state identification card or driver's license number but does not include a government-issued identifier required by law to be displayed in public;

(B) Any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition, or treatment of an individual, and includes, but is not limited to, gender-affirming health data, reproductive or sexual health data, legally-protected health care data, and neural data;

(C) A consumer's tax return and account number, financial account number, debit card number, credit card number, or information that describes or reveals the income level, indebtedness, or bank account balances of an individual;

(D) Biometric data or genetic information or information derived therefrom;

(F) Precise geolocation information;

(G) An individual's private communications such as voicemails, emails, texts, direct messages, mail, voice communications, and video communications, or information identifying the parties to such communications or pertaining to the transmission of such communications, including telephone numbers called, telephone numbers from which calls were placed, the time

calls were made, call duration, and location information of the parties to the call. Communications are not private for purposes of this sub-paragraph if such communications are made from or to a device provided by an employer to an employee insofar as such employer provides conspicuous notice that such employer may access such communications;

(H) Account or device log-in credentials, or security or access codes for an account or device;

(I) Information identifying the sexual behavior of an individual;

(J) Calendar information, address book information, phone or text logs, photos, audio recordings, or videos, maintained for private use by an individual, regardless of whether such information is stored on the individual's device or is accessible from that device and is backed up in a separate location. Such information is not sensitive for purposes of this sub-paragraph if such information is sent from or to a device provided by an employer to an employee insofar as such employer provides conspicuous notice that it may access such information;

(L) Information revealing the video content requested or selected by an individual. This clause does not include personal data used solely for transfers for independent video measurement;

(M) Personal data of an individual when a controller or processor knows or should have known that an individual is a minor;

(N) An individual's race, color, ethnicity, religion, national origin, citizenship, immigration status, philosophical beliefs, or union membership;

(O) Information identifying an individual's online activities over time and across websites, online applications, or mobile applications that do not share common branding, or data generated by profiling performed on such data;

(P) Information that reveals the status of an individual as a veteran, or member of the military division established under chapter 33 or Armed Forces of the United States;

(Q) Information that reveals an individual's sexual orientation, or status as transgender or non-binary;

(R) Information that reveals the status of an individual as a victim of a crime;

(S) An individual's keystrokes;

(T) An individual's driving behavior;

(U) social care information that is stored in or transmitted through a closed-loop referral system; or

(V) Any other data collected, processed, or transferred for the purpose of identifying the types of personal data listed in subparagraphs (A) through (U), inclusive.

(48) "Small business" means a controller or processor that meets the following criteria for the period of the 3 preceding calendar years (or for the period during which the controller or processor has been in existence if such period is less than 3 years):

(A) The controller or processor' average annual gross revenues during the period did not exceed $20,000,000;

(B) The controller or processor, on average, did not annually collect, process, retain, or transfer the personal data of more than 200,000 individuals during the period for any purpose other than initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product; and

(C) The controller or processor did not transfer personal data to a third party in exchange for revenue or other valuable consideration, except for purposes of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product.

(49) "Social care" means care, services, goods, or supplies related to an individual's social needs. "Social care" includes, but is not limited to, support and assistance for an individual's food stability and nutritional needs, housing, transportation, economic stability, employment, education access and quality, child care and family relationship needs, and environmental and physical safety.

(50) "Social care information" means any information that relates to the need for, payment for, or provision of social care, and identifies the person receiving social care, or for which there is a reasonable basis to believe the information can be used to identify the individual receiving social care.

(51) "Targeted advertising" means displaying or presenting an online advertisement to a consumer or to a device identified by a unique persistent identifier, or to a group of consumers or devices identified by unique persistent identifiers, if the advertisement is selected based, in whole or in part, on known or predicted preferences, characteristics, behavior, or interests associated with the consumer or a device identified by a unique persistent identifier.

“Targeted advertising” includes displaying or presenting an online advertisement for a product or service based on the previous interaction of a consumer or a device identified by a unique persistent identifier with such product or service on a website or online service that does not share common branding with the website or online service displaying or presenting the advertisement, and marketing measurement related to such advertisements.

“Targeted advertising” does not include:

(A) first-party advertising; or

(B) contextual advertising.

(52) “Third party” means a person that collects personal data from another person that is not the consumer to whom the data pertains and is not a processor with respect to such data.

“Third party” does not include a person that collects personal data from another entity if the two entities are affiliates.

(53) “Trade secret” has the same meaning as provided in section 42 of chapter 93.

(54) “Transfer” means to disclose, release, disseminate, make available, license, rent, or share personal data to a third party orally, in writing, electronically, or by any other means.

(55) "Unique persistent identifier" means a technologically created identifier to the extent that such identifier is reasonably linkable to a consumer or a device that identifies or is linked or reasonably linkable to 1 or more consumers, including device identifiers, Internet Protocol addresses, cookies, beacons, pixel tags, mobile ad identifiers or similar technology customer numbers, unique pseudonyms, user aliases, telephone numbers, or other forms of persistent or probabilistic identifiers that are linked or reasonably linkable to 1 or more consumers or devices.

The term "unique persistent identifier" does not include an identifier assigned by a controller for the sole purpose of giving effect to the exercise of affirmative consent or opt out by a consumer with respect to the collecting, processing, and transfer of personal data or otherwise limiting the collecting, processing, or transfer of personal data.

Section 2. Applicability.

The provisions of this chapter apply to persons that conduct business in this state or persons that produce products or services that are targeted to residents of this state and that during the preceding calendar year:

(a) Collected or processed the personal data of not less than 25,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction, so long as all personal data collected or processed for such purpose was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a business's return policy; or

(b) derived revenue or other valuable consideration from the sale of personal data.

Section 3. Scope.

(a) The provisions of this chapter do not apply to (1) any Federal, State, Tribal, territorial, or local government entity such as a body, authority, board, bureau, commission, district or agency of the Commonwealth or of any political subdivision of the Commonwealth; (2) a nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance, and is operating solely for that purpose; (3) a national securities association registered pursuant to § 15A of the Securities Exchange Act of 1934 (15 U.S.C. § 78a, et seq., as amended)

and the rules and implementing regulations promulgated thereunder, and operating solely for that purpose; and (4) a registered futures association so designated pursuant to § 17 of the Commodity Exchange Act (7 U.S.C. § 1, et seq., as amended) and the rules and implementing regulations promulgated thereunder, and operating solely for that purpose.

(b) The following information and data is exempt from the provisions of this chapter, provided only if said information and data is processed, collected, or transferred, as applicable, in compliance with the federal statutes or regulations referenced, if any, in each exemption under this paragraph:

(1) protected health information that a covered entity or business associate collects or processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with HIPAA and regulations promulgated under HIPAA;

(2) patient-identifying information for purposes of 42 USC 290dd-2, as amended from time to time;

(3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 CFR 46;

(4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;

(5) the protection of human subjects under 21 CFR Parts 6, 50 and 56, or personal data used or shared in research, as defined in 45 CFR 164.501, that is conducted in accordance with

the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law;

(6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq. as amended from time to time;

(7) patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as amended from time to time;

(8) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

(9) Personal information collected, processed, or sold subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq. as amended from time to time;

(10) personal data collected, processed, sold or disclosed subject to the Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended from time to time;

(11) personal data regulated by the Family Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended from time to time;

(12) data collected, processed, or maintained:

(A) in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role,

(B) as the emergency contact information of an individual under this chapter used for emergency contact purposes, or;

(C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subdivision (1) of this subsection and used for the purposes of administering such benefits.

(c) Controllers and processors that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to this chapter.

Section 4. Consumer rights.

(a) A consumer shall have the right to:

(1) Confirm whether or not a controller is collecting or processing the consumer's personal data, including, but not limited to, any inferences about the consumer derived from such personal data, and access such personal data;

(2) obtain from a controller a list of specific third parties, other than natural persons, to which the controller has transferred either (i) the consumer’s personal data; or (ii) any personal data;

(3) correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data, and instruct a controller or processor to make reasonable efforts to notify all third parties or processors to which the controller has transferred such personal data of such corrections;

(4) delete personal data provided by, or obtained about, the consumer, including personal data the consumer provided to the controller, personal data the controller obtained from another source, and derived data and instruct a controller or processor to make reasonable efforts to notify all third parties or processors to which the controller has transferred such personal data of such deletion request;

(5) obtain a copy of the consumer's personal data collected or processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and

(6) opt out of the collection and processing of the personal data for purposes of

(A) targeted advertising;

(B) the transfer of personal data; or

(C) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(b)(1) If a consumer’s personal data is profiled in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer, the consumer has the right to question the result of such profiling, to be informed of the reason why the profiling resulted in the decisions, and, if feasible, to be informed of what actions the consumer might have taken to secure a different decisions and the actions that the consumer might take to secure a different decision in the future.

(2) The consumer has the right to review the consumer’s personal data used in the profiling.

(3) If the decision is determined to have been based upon inaccurate personal data, the consumer has the right to have the data corrected and the profiling decision revaluated based upon the corrected data.

(c) A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 5 of this chapter to exercise the rights of such consumer specified in this section on behalf of the consumer. In the case of personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf. In the case of personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

(d) Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized in this chapter as follows:

(1) A controller shall respond to the consumer without undue delay, but not later than forty-five days after receipt of the request. The controller may extend the response period once by twenty additional days when reasonably necessary, considering the complexity and number of the consumer's requests, provided the controller informs the consumer of any such extension within the initial forty-five-day response period and of the reason for the extension.

(2) If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than forty-five days after receipt of

the request, of the justification for declining to take action and instructions for how to appeal the decision.

(3) Information provided in response to a consumer request shall be provided by a controller, free of charge, twice per consumer during any twelve-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

(4) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (1) to (5), inclusive, of subsection (a) of this section using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise such right or rights until such consumer provides additional information reasonably necessary to authenticate such consumer and such consumer's request to exercise such right or rights, provided that any such information may not be used for any purposes other than the authentication of such consumer. A controller shall not require authentication to exercise an opt-out request, but a controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request disclosing that such controller believes such request is fraudulent, why such controller believes such request is fraudulent and that such controller shall not comply with such request. If the request was placed through an agent, both the agent and the person who appointed the agent shall receive that notice.

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete such data pursuant to subdivision (4) of subsection (a) of this section by deleting the consumer's personal data retained by the controller and retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the controller's records and not using such retained data for any other purpose pursuant to this chapter.

(d) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than sixty days after receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

(e) A controller may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a right described in this section through:

(1) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(2) the use of dark patterns or deceptive design.

(f) A controller or processor may not collect, process, or transfer personal data in a manner that discriminates against, or threaten to discriminate against, an individual or class of individuals, or otherwise makes unavailable the equal enjoyment of goods or services, on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, sex, sexual orientation, gender identity, gender expression, physical or mental disability, religion, genetic information, pregnancy or condition related to pregnancy, status as a veteran, ancestry, national origin, citizenship, immigration status, or any other basis protected by chapter 151B.

(g) Subsection (f) does not apply to:

(1) The collection, processing, or transfer of personal data for the sole purpose of:

(A) A controller or processor's self-testing to prevent or mitigate unlawful discrimination or otherwise to ensure compliance with Massachusetts or federal law; or

(B) Diversifying an applicant, participant or customer pool; or

(2) A private establishment, as described in 42 United States Code, Section 2000a(e).

Section 5. Authorized agent.

(a) A consumer may designate another person to serve as the consumer's authorized agent, and act on such consumer's behalf, to exercise rights specified in subsection (a) of section 4 of this chapter. A controller shall comply with a request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on such consumer's behalf.

(b) An individual may designate an authorized agent as provided in subsection (a) by technological means, including, but not limited to, an Internet link or a browser setting, browser

extension or global device setting that indicates the individual's intent to opt out processing for one or more of the purposes specified in section 4.

Section 6. Actions of controllers.

(a) A controller shall:

(1) Limit the collection, processing, and transfer of personal data to what is reasonably necessary to provide or maintain:

(A) a specific product or service requested by the consumer to whom the data pertains including any routine administrative, operational, or account-servicing activity, such as billing, shipping, delivery, storage, or accounting; or

(B) a communication, that is not an advertisement, by the controller to the consumer reasonably anticipated within the context of the relationship between the controller and the consumer.

Except with respect to sensitive data, a controller may process or transfer personal data collected under this subsection to provide first-party advertising or targeted advertising; provided, however, that this paragraph does not permit the processing or transfer of personal data for targeted advertising to a consumer who has opted out of such advertising pursuant to section 4, 5, or 6, or to a consumer under circumstances where the controller knows or should have known that the consumer is a minor;

(2) not collect, process, or transfer sensitive data concerning a consumer except when such collection, processing, or transfer is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the sensitive data pertains;

(3) not sell sensitive data;

(4) establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue, including disposing of personal data in accordance with a retention schedule that requires the deletion of personal data when the data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected, processed, or transferred;

(5) not transfer sensitive data concerning a consumer without obtaining the consumer's affirmative consent, or, in the case of the collection or processing of personal data concerning a known child, without collecting or processing such data in accordance with COPPA;

(6) provide an effective mechanism for a consumer, that does not use dark patterns or deceptive design, to revoke the consumer's affirmative consent under this chapter that is at least as easy as the mechanism by which the consumer provided the consumer's affirmative consent and, upon revocation of such affirmative consent, cease to process the data as soon as practicable, but not later than fifteen days after the receipt of such request;

(7) not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer's personal data, under circumstances where a controller knows or should have known, that the consumer is a minor; and

(8) not discriminate or retaliate against, or threaten to 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.

(b) Nothing in paragraph (8) of subsection (a) shall be construed to require a controller to provide a product or service that requires the personal data of a consumer which the controller does not collect or maintain, or prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a financial incentive program such as a bona fide loyalty, rewards, premium features, discounts or club card program, provided that the controller may not transfer personal data to a third party as part of such program unless:

(1) The transfer is functionally necessary to enable the third party to provide a benefit to which the consumer is entitled;

(2) the transfer of personal data to the third party is clearly disclosed in the terms of the program; and

(3) the third party uses the personal data only for purposes of facilitating a benefit to which the consumer is entitled and does not process or transfer the personal data for any other purpose.

The sale of personal data shall not be considered functionally necessary to provide a financial incentive program. A controller shall not use financial incentive practices that are unjust, unreasonable, coercive or usurious in nature.

(c) (1) A controller shall provide consumers with a reasonably accessible, understandable, clear and meaningful and not misleading privacy notice that includes a detailed and accurate representation of:

(i) The categories of personal data collected and processed by the controller, including a separate list of categories of sensitive data collected and processed by the controller, described in a level of detail that provides consumers a meaningful understanding of the type of personal data collected or processed;

(ii) the purpose for collecting and processing each category of personal data the controller collects or processes described in a way that gives consumers a meaningful understanding of how each category of their personal data will be use;

(iii) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;

(iv) the categories of personal data that the controller transfers to third parties, if any, and the purposes for those transfers;

(v) the categories of third parties, if any, to which the controller transfers personal data including the name of each data broker to which the controller transfers personal data;

(vi) The length of time the controller intends to retain each category of personal data, or, if it is not possible to identify the length of time, the criteria used to determine the length of time the controller intends to retain categories of personal data; and

(vii) an active electronic mail address or other online mechanism that the consumer may use to contact the controller for privacy and data security inquiries.

(viii) identifies the controller, including any business name under which the controller registered with the Secretary of State and any assumed business name that the controller uses in Massachusetts;

(ix) describes any collection, processing, selling, or sharing of personal data for training or use of artificial intelligence systems, if applicable;

(x) provides a clear and conspicuous description of any processing of personal data in which the controller engages for the purposes of targeted advertising, sale of personal data to third parties, or profiling the consumer in furtherance of decisions that produce legal or similarly significant effects concerning the consumer, and a procedure by which the consumer may opt out of this type of processing;

(xi) a general description of the controller's data security practices; and

(xii) the effective date of the privacy notice.

(2)(i) The privacy notice shall be provided directly to consumers and made available online to the general public.

(ii) The privacy notice must be provided in a manner that is reasonably accessible to and usable by individuals with disabilities. The notice shall be made available to the public in each covered language in which the controller provides a product or service that is subject to the privacy notice; or carries out activities related to such product or service.

(iii) If a controller makes a material change to its privacy notice, the controller shall notify each consumer affected by the material change before implementing the material change with respect to prospectively collected personal data and provide a reasonable opportunity for

each consumer to withdraw consent. A controller shall provide a reasonable opportunity for each consumer to affirmatively consent to further materially different collection, processing or transfer of previously collected personal data under the changed notice. The controller shall take all reasonable electronic measures to provide direct notification regarding material changes to the privacy notice to each affected consumer, in each covered language in which the privacy notice is made available, taking into account available technology and the nature of the relationship.

(iv) Each large data holder shall retain copies of previous versions of its privacy notice for at least 10 years beginning after the date of enactment of this chapter and publish them on its website. Such large data holder shall make publicly available, in a clear, conspicuous, and readily accessible manner, a log describing the date and nature of each material change to its privacy notice over the past 10 years. The descriptions shall be sufficient for a reasonable individual to understand the material effect of each material change. The obligations in this paragraph shall not apply to any previous versions of a large data holder's privacy notice, or any material changes to such notice, that precede the date of enactment of this chapter.

(v) In addition to the privacy notice required under this paragraph, a large data holder that is a controller shall provide a short form notice of no more than 500 words in length that includes the main features of their data practices.

(vi) Each controller that collects, processes, or transfers biometric data shall provide a separate privacy notice detailing the collection, processing, and transfer of such biometric data, subject to the provisions of paragraphs (1) and (2) of this section.

(vii) Each controller that collects, processes, or transfers specific precise geolocation information shall provide a separate privacy notice detailing the collection, processing, and

transfer of such precise geolocation information, subject to the provisions of paragraphs (1) and (2) of this section.

(d) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose such sales or processing, as well as the manner in which a consumer may exercise the right to opt out of such sales or processing.

(e) A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights pursuant to this chapter. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to verify the identity of the consumer making the request. A controller shall not require a consumer to create a new account in order to exercise consumer rights, but may require a consumer to use an existing account. Any such means shall include:

(1) Providing a clear and conspicuous link on the controller's Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising, the sale of the consumer's personal data, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer; and

(2) Not later than 18 months after the effective date of this chapter, allowing a consumer to opt out of any collection or processing of the consumer's personal data for the purposes of targeted advertising, or any sale of the consumer’s personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the

controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology or mechanism shall:

(i) Be consumer-friendly and easy to use by the average consumer;

(ii) Not use dark patterns or deceptive design; and

(iii) Enable the controller to reasonably determine whether the consumer is a resident of this state and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising. For purposes of this subsection, the use of an internet protocol address to estimate the consumer’s location shall be considered sufficient to reasonably determine residency.

If a consumer's decision to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of personal data, through an opt-out preference signal sent in accordance with the provisions of this subsection conflicts with the consumer's existing controller-specific privacy setting or voluntary participation in a controller's financial incentive program, the controller shall comply with such consumer's opt-out preference signal but may notify such consumer of such conflict and provide to such consumer the choice to confirm such controller-specific privacy setting or participation in such program.

(f) If a controller responds to consumer opt-out requests received pursuant to subsection (e) of this section by informing the consumer of a change in the price, rate, level, quality, or selection of goods or services, the controller shall present the terms of any financial incentive offered pursuant to subsection (b) of this section for the retention, processing, sale or transfer of the consumer's personal data.

Section 7. Responsibilities of processors and controllers.

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter. Such assistance shall include:

(1) Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, insofar as is reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests;

(2) taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of the system of the processor, in order to meet the controller's obligations; and

(3) providing necessary information to enable the controller to conduct and document data protection assessments.

(b) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be written, binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties including a method by which the processor shall notify the controller of material changes to its privacy practices. The processor shall adhere to the instructions of the controller and only process and transfer the data it receives from the controller to the extent necessary to provide a service requested by the controller, as set out in the contract. The contract shall also require that the processor:

(1) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

(2) at the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(3) upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

(4) after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the contractual and statutory or regulatory obligations of the processor with respect to the personal data;

(5) be prohibited from combining personal data that the processor receives from or on behalf of a controller with personal data that the processor receives from or on behalf of another person or collects from the interaction of the processor with an individual; and

(6) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request.

(c) A processor shall establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data that are consistent with chapter 93H and appropriate to the volume and nature of the personal data at issue.

(d) Nothing in the contract in subsection (b) shall relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of such controller's or processor's role in the processing relationship, as described in this chapter.

(e) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in such person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to such instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to such processing and may be subject to an enforcement action under this chapter.

(f) A processor shall not process or transfer personal data on the behalf of a controller if the processor knows or should have known that the controller has violated this chapter with respect to such personal data.

Section 8. Data Protection Assessments.

(a) A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment for each of the

controller's processing activities that presents such heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:

(1) The collection or processing of personal data for the purposes of targeted advertising;

(2) the sale of personal data;

(3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of:

(A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers,

(B) financial, physical or reputational injury to consumers,

(C) 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

(D) other substantial injury to consumers; and

(4) the collection or processing of sensitive data.

(b) Data protection assessments conducted pursuant to subsection (a) of this section shall identify the categories of personal data collected, the purposes for collecting such personal data, whether personal data is being transferred, and identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that are employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data

and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) No later than 30 days after completing a data protection assessment under this section, a controller shall submit a report of the data protection assessment or evaluation to the Attorney General. The report must include a summary of the data protection assessment and the controller shall make the summary publicly available in a place that is easily accessible to consumers. Controllers may redact trade secrets or other confidential or proprietary information from the report, provided that notwithstanding the foregoing, the Attorney General may require that a controller disclose any data protection assessment, and any information contained therein, that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment, and said information, available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in this chapter. To the extent any information contained in a data protection assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment is

reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(f) A controller shall conduct and document a data protection assessment before initiating a processing activity that presents a heightened risk of harm to a consumer and shall review and update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of personal data collected or processed and level of risk presented by the processing, throughout the processing activity's lifecycle in order to:

(1) monitor for harm caused by the processing and adjust safeguards accordingly; and

(2) ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing.

(g) A controller or processor shall establish, implement, and maintain reasonable policies, practices, and procedures that reflect the role of the controller or processor in the collection, processing, and transferring of personal data and that:

(1) consider applicable federal and Massachusetts laws, rules, or regulations related to personal data the controller or processor collects, processes, or transfers;

(2) identify, assess, and mitigate privacy risks related to minors;

(3) mitigate privacy risks related to the products and services of the controller or processor, including in the design, development, and implementation of such products and services, considering the role of the controller or processor and the information available to it;

(4) evaluate the length of time that personal data shall be retained and circumstances under which personal data shall be deleted, de-identified, or otherwise modified with respect to the purposes for which it was collected or processed and the sensitivity of the personal data; and

(5) implement reasonable training and safeguards within the controller or processor to promote compliance with all privacy laws applicable to personal data the controller collects, processes, or transfers or personal data the processor collects, processes, or transfers on behalf of the controller and mitigate privacy risks taking into account the role of the controller or processor and the information available to it.

(h) The policies, practices, and procedures established by a controller or processor under subsection (g), shall correspond with, as applicable:

(1) the size of the controller or processor and the nature, scope, and complexity of the activities engaged in by the controller or processor, including whether the controller or processer is a large data holder, nonprofit organization, small business, third party, or data broker, considering the role of the controller or processor and the information available to it;

(2) the sensitivity of the personal data collected, processed, or transferred by the controller or processor;

(3) the volume of personal data collected, processed, or transferred by the controller or processor;

(4) the number of individuals and devices to which the personal data collected, processed, or transferred by the controller or processer relates; and

(5) the cost of implementing such policies, practices, and procedures in relation to the risks and nature of the personal data.

Section 9. De-identified data.

(a) Any controller in possession of de-identified data shall:

(1) Take technical measures to ensure that the data cannot be associated with an individual;

(2) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

(3) contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter.

(b) Nothing in this chapter shall be construed to:

(1) Require a controller or processor to re-identify de-identified data; or

(2) maintain data in identifiable form, or collect, obtain, retain or access any data or technology, in order to be capable of associating an authenticated consumer request with personal data.

(c) Nothing in this chapter shall be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

(1) Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data; and

(2) does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer;

(d) A controller that transfers de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

Section 10. Limitations.

(a) Nothing in this chapter shall be construed to restrict a controller's or processor's ability to:

(1) Comply with federal or other Massachusetts laws;

(2) comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, or Massachusetts state, municipal or other governmental authorities;

(3) cooperate with federal or Massachusetts law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal or Massachusetts law

(4) investigate, establish, exercise, prepare for or defend legal claims;

(5) provide a product or service specifically requested by the consumer;

(6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(7) take steps at the request of a consumer prior to entering into a contract;

(8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis;

(9) prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity targeted at or involving the controller or processor or its services, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action, provided that for the purposes of this paragraph, "illegal activity" means a violation of a federal, state, or local law punishable as a felony or misdemeanor that can directly harm;

(10) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all relevant laws and regulations governing such research, if applicable, and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine,

(A) whether the deletion of personal data requested by a consumer under section 4, subsection (a), subparagraph (4) is likely to provide substantial benefits that do not exclusively accrue to the controller,

(B) the expected benefits of the research outweigh the privacy risks, and

(C) whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

(11) assist another controller, processor or third party with any of the obligations under this chapter;

(12) process personal data for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is

(A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed, and

(B) under the responsibility of a professional subject to confidentiality obligations under federal, state or local law;

(13) ensure the data security and integrity of personal data as required by this chapter, protect against spam, or protect and maintain networks and systems, including through diagnostics, debugging, and repairs;

(14) transfer assets 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:

(A) A notice describing the transfer, including the name of the entity receiving the consumer's personal data and the applicable privacy notices of such entity and

(B) a reasonable opportunity to:

(i) withdraw previously provided consent related to the consumer's personal data, and

(ii) request the deletion of the consumer's personal data;

(15) effectuate a product recall pursuant to federal or state law, or to fulfill a warranty;

(16) conduct medical research in compliance with part 46 of title 45, Code of Federal Regulations, or parts 50 and 56 of title 21, Code of Federal Regulations

(17) publish entity-based member or employee contact information where such publication is intended to allow members of the public to contact such member or employee in the ordinary course of the entity's operations; or

(18) process personal data previously collected in accordance with this chapter such that the personal data becomes de-identified data, including to:

(A) Conduct internal research to develop, improve or repair products, services or technology;

(B) identify and repair technical errors that impair existing or intended functionality; or;

(C) perform solely internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(b) The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor with said sections would violate an evidentiary privilege under the laws of this state. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of the state as part of a privileged communication.

(d) Nothing in this chapter shall be construed to:

(1) Impose any obligation on a controller or processor that adversely affects the rights or freedoms of any person, including, but not limited to, the rights of any person to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution or Article 16 of the Massachusetts Declaration of Rights;

(2) apply to any person's collection or processing of personal data in the course of such person's purely personal or household activities; or

(3) for private schools approved under section 1 of chapter 76 and private institutions of higher education as defined by title I of the Higher Education Act of 1965, 20 United States Code, Section 1001 et seq., require deletion of personal data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution.

(4) for a consumer reporting agency, as defined in 15 U.S.C. 1681a(f), require deletion of personal data used for the purpose of evaluating a consumer’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living, subject to the provisions of the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.

(e) Personal data collected or processed by a controller pursuant to this section may be collected or processed to the extent that such collection and processing is:

(1) Reasonably necessary and proportionate to the purposes listed in this section, or, in the case of sensitive data, strictly necessary to the purposes listed in this section;

(2) limited to what is necessary in relation to the specific purposes listed in this section. Personal data processed pursuant to subsection (b) of this section shall, where applicable, take

into account the nature and purpose or purposes of such processing. Such data shall be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such processing of personal data; and

(3) compliant with section 4, subsection (f).

(f) If a controller collects or processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such collection or processing qualifies for the exemption and complies with the requirements in subsection (e) of this section.

Section 11. Rulemaking.

The Attorney General may adopt, amend, or rescind rules and regulations for the implementation, administration, and enforcement of this chapter.

Section 12. Enforcement.

(a) The Attorney General may bring a civil action against a controller or processor 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 and obtain 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 obtained directly or indirectly by any such violation on behalf of the residents of the Commonwealth or individuals present in the Commonwealth; (4) impose civil penalties in an amount not less than $15,000 per individual per violation, as adjusted annually to reflect an increase in the Consumer Price Index;

(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.

(b) A violation of this chapter or a regulation adopted under this chapter with respect to the personal data of a consumer constitutes an injury to that consumer. The injured consumer may bring a civil action against the party that commits the violation, provided such party is not a small business. In a civil action brought under this subsection in which a plaintiff prevails, the court may award the plaintiff:

(1) Damages in an amount not less than $15,000 per individual per violation, as adjusted annually to reflect an increase in the Consumer Price Index, or actual damages, whichever is greater;

(2) punitive damages;

(3) injunctive relief, including an order that an entity retrieve any personal data transferred in violation of this chapter or a regulation adopted under this chapter;

(4) declaratory relief; or

(5) reasonable attorney's fees and litigation costs.

(c) When calculating awards and civil penalties in any action under this section, the court shall consider:

(1) the number of affected individuals and the amount and sensitivity of any personal data at issue;

(2) the severity of the violation or noncompliance;

(3) the risks caused by the violation or noncompliance;

(4) whether the violation or noncompliance was part of a pattern of noncompliance and violations and not an isolated instance;

(5) whether the violation or noncompliance was willful and not the result of error;

(6) the precautions taken by the defendant to prevent a violation;

(7) the number of administrative actions, lawsuits, settlements, and consent-decrees under this chapter involving the defendant;

(8) the number of administrative actions, lawsuits, settlements, and consent-decrees involving the defendant in other states and at the federal level in issues involving information privacy; and

(9) the international record of the defendant when it comes to information privacy issues.

(d) A violation of the requirements of this chapter, or a regulation adopted under this chapter, constitutes an unfair or deceptive practice in the conduct of trade or commerce for the purposes of chapter 93A.

(e) Any provision of a contract or agreement of any kind, including but not limited to a controller's terms of service or a privacy notice, including the short-form privacy notice required under section 15 subsection (h), 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 public policy and shall be void and unenforceable.

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

(h) Notwithstanding paragraph A of section 99 of chapter 272, a person who willfully violates this chapter shall be punished to the same extent as a violation of subparagraph (3) of paragraph C of said section.

Section 13. Relationship to Other Laws.

(a) Nothing in this chapter shall diminish any individual's rights or obligations under chapters 66A, 93A, 93H, 151B, or under sections 1B or 3B of chapter 214.

(b) In a conflict between chapter 175I and this chapter, this chapter shall control.

Section 14. Targeted Advertising to Minors.

A controller shall not engage in targeted advertising or first-party advertising to a consumer if the controller knows or should have known that the consumer is a minor.

Section 15. Data Brokers Annual Registration.

(a) Annually, on or before January 31 following a year in which a person meets the definition of data broker, a data broker shall:

(1) register with the OCABR;

(2) pay a registration fee of $100.00; and

(3) provide the following information:

(A) the name and primary physical, e-mail, and internet addresses of the data broker;

(B) if the data broker permits a consumer to opt out of the data broker's collection of brokered personal information, opt out of its databases, or opt out of certain sales of data:

(i) the method for requesting an opt-out;

(ii) if the opt-out applies to only certain activities or sales, which ones; and

(iii) whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;

(C) a statement specifying the data collection, databases, or sales activities from which a consumer may not opt out;

(D) a statement whether the data broker implements a purchaser credentialing process;

(E) the number of data broker security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;

(F) where the data broker has knowledge that it possesses the brokered personal information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors; and

(G) any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(b) A data broker that fails to register pursuant to subsection (a) of this section is liable to the Commonwealth for:

(1) a civil penalty of $125.00 for each day it fails to register pursuant to this section;

(2) an amount equal to the fees due under this section during the period it failed to register pursuant to this section; and

(3) other penalties imposed by law.

(c) A data broker that omits required information from its registration shall file an amendment to include the omitted information within 30 business days following notification of the omission and is liable to the Commonwealth for a civil penalty of $1,000.00 per day for each day thereafter.

(d) A data broker that files materially incorrect information in its registration:

(1) is liable to the Commonwealth for a civil penalty of $25,000.00; and

(2) if it fails to correct the false information within 30 business days after discovery or notification of the incorrect information, an additional civil penalty of $1,000.00 per day for each day thereafter that it fails to correct the information.

Section 16. Data Broker Opt Out.

(a) By January 1, 2027, the OCABR shall either partner with the California Privacy Protection Agency to make available California's accessible deletion mechanism for Massachusetts consumers, in which case a data broker's compliance with said mechanism for Massachusetts consumers shall satisfy the requirements of this paragraph, or establish an accessible deletion mechanism that does all of the following:

(1) Implements and maintains reasonable security procedures and practices, including, but not limited to, administrative, physical, and technical safeguards appropriate to the nature of the information and the purposes for which the personal data will be used and to protect consumers' personal data from unauthorized use, disclosure, access, destruction, or modification.

(2) Allows a consumer, through a single verifiable consumer request, to request that every data broker that maintains any personal data delete any personal data related to that consumer held by the data broker or associated service provider or contractor.

(3) Allows a consumer to selectively exclude specific data brokers from a request made under paragraph (2).

(4) Allows a consumer to make a request to alter a previous request made under this subdivision after at least 45 days have passed since the consumer last made a request under this subdivision.

(b) The accessible deletion mechanism established pursuant to subdivision (a) shall meet all of the following requirements:

(1) The accessible deletion mechanism shall allow a consumer to request the deletion of all personal data related to that consumer through a single deletion request.

(2) The accessible deletion mechanism shall permit a consumer to securely submit information in one or more privacy-protecting ways determined by the OCABR to aid in the deletion request.

(3) The accessible deletion mechanism shall allow data brokers registered with the OCABR to determine whether an individual has submitted a verifiable consumer request to delete the personal data related to that consumer as described in paragraph (1) and shall not allow the disclosure of any additional personal data when the data broker accesses the accessible deletion mechanism unless otherwise specified in this title.

(4) The accessible deletion mechanism shall allow a consumer to make a request described in paragraph (1) using an internet service operated by the OCABR.

(5) The accessible deletion mechanism shall not charge a consumer to make a request described in paragraph (1).

(6) The accessible deletion mechanism shall allow a consumer to make a request described in paragraph (1) in any language spoken by any consumer for whom personal data has been collected by data brokers.

(7) The accessible deletion mechanism shall be readily accessible and usable by consumers with disabilities.

(8) The accessible deletion mechanism shall support the ability of a consumer's authorized agents to aid in the deletion request.

(9) The accessible deletion mechanism shall allow the consumer, or their authorized agent, to verify the status of the consumer's deletion request.

(10) The accessible deletion mechanism shall provide a description of all of the following:

(A) The deletion permitted by this section, including, but not limited to, the actions required by subdivisions (c) and (d).

(B) The process for submitting a deletion request pursuant to this section.

(C) Examples of the types of information that may be deleted.

(c) (1) Beginning August 1, 2027, a data broker shall access the accessible deletion mechanism established pursuant to subdivision (a) at least once every 45 days and do all of the following:

(A) Within 45 days after receiving a request made pursuant to this section, process all deletion requests made pursuant to this section and delete all personal data related to the consumers making the requests consistent with the requirements of this section.

(B) In cases where a data broker denies a consumer request to delete under this title because the request cannot be verified, process the request as an opt-out of the sale or sharing of the consumer's personal data, as provided under this chapter.

(C) Direct all service providers or contractors associated with the data broker to delete all personal data in their possession related to the consumers making the requests described in subparagraph (A).

(D) Direct all service providers or contractors associated with the data broker to process a request described by subparagraph (B) as an opt-out of the sale or sharing of the consumer's personal data, as provided under this chapter.

(2) Notwithstanding paragraph (1), a data broker shall not be required to delete a consumer's personal data if either of the following apply:

(A) It is reasonably necessary for the data broker to maintain the personal data to fulfill a purpose described in section 10.

(B) The deletion is not required under this chapter.

(3) Personal information described in paragraph (2) shall only be used for the purposes described in paragraph (2) and shall not be used or disclosed for any other purpose, including, but not limited to, marketing purposes.

(d) (1) Beginning August 1, 2027, after a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant to this section, the data broker shall delete all personal data of the consumer at least once every 45 days pursuant to this section unless the consumer requests otherwise or the deletion is not required pursuant to paragraph (2) of subdivision (c).

(2) Beginning August 1, 2027, after a consumer has submitted a deletion request and a data broker has deleted the consumer's data pursuant to this section, the data broker shall not sell

or share new personal data of the consumer unless the consumer requests otherwise or selling or sharing the personal data is permitted under this chapter.

(e) (1) Beginning January 1, 2028, and every three years thereafter, a data broker shall undergo an audit by an independent third party to determine compliance with this section.

(2) For an audit completed pursuant to paragraph (1), the data broker shall submit a report resulting from the audit and any related materials to the OCABR within five business days of a written request from the OCABR.

(3) A data broker shall maintain the report and materials described in paragraph (2) for at least six years.

(f) (1) The OCABR may charge an access fee to a data broker when the data broker accesses the accessible deletion mechanism pursuant to subdivision (d) that does not exceed the reasonable costs of providing that access.

Section 17. Data Broker Credentialing.

(1) A data broker shall maintain reasonable procedures designed to ensure that the brokered personal data it discloses is used for a legitimate and legal purpose.

(2) These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information shall be used for no other purpose.

(3) A data broker shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by the prospective user prior to furnishing the user brokered personal data.

(4) A data broker shall not furnish brokered personal data to any person if it has reasonable grounds for believing that the brokered personal data will not be used for a legitimate and legal purpose.

SECTION 2. The General Laws, as appearing in the 2022 Official Edition, are hereby amended by inserting after chapter 93M the following chapter:

Chapter 93N. Location Shield Act.

Section 1. Definitions

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

(1) "Collect", to obtain, infer, generate, create, receive, or access an individual's location information.

(2) "Consent", freely given, specific, informed, unambiguous, opt-in consent. This term does not include either of the following: (i) agreement secured without first providing to the individual a clear and conspicuous disclosure of all information material to the provision of consent, apart from any privacy policy, terms of service, terms of use, general release, user agreement, or other similar document; or (ii) agreement obtained through the use of a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

(3) "Covered entity", any individual, partnership, corporation, limited liability company, association, or other 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. A covered entity does not include an individual acting in a non-commercial context. A covered entity includes all agents of the entity.

(5) “Device”, a mobile telephone, as defined in section 1 of chapter 90 of the general laws, or any other electronic device that is or may commonly be carried by or on an individual and is capable of connecting to a cellular, bluetooth, or other wireless network.

(6) “Disclose”, to make location information available to a third party, including but not limited to by sharing, publishing, releasing, transferring, disseminating, providing access to, or otherwise communicating such location information orally, in writing, electronically, or by any other means.

(7) “Individual”, a person located in the Commonwealth of Massachusetts.

(8) “Location information”, information derived from technology, including but not limited to, a device or from interactions between devices, with or without the knowledge of the user and regardless of the technological method used, that pertains to or directly or indirectly reveals the present or past geographical location of an individual or device within the Commonwealth of Massachusetts with sufficient precision to identify street-level location information within a range of 1,850 feet or less. Location information includes but is not limited to (i) an internet protocol address capable of revealing the physical or geographical location of an individual; (ii) Global Positioning System (GPS) coordinates; and (iii) cell-site location information. This term does not include location information identifiable or derived solely from the visual content of a legally obtained image, including the location of the device that captured such image, or publicly posted words.

(9) “Location Privacy Policy”, a description of the policies, practices, and procedures controlling a covered entity’s collection, processing, management, storage, retention, and deletion of location information.

(10) “Monetize”, to collect, process, or disclose an individual’s location information for profit or in exchange for monetary or other consideration. This term includes but is not limited to selling, renting, trading, or leasing location information.

(11) “Person”, any natural person.

(12) “Permissible purpose”, one of the following purposes: (i) provision of a product, service, or service feature to the individual to whom the location information pertains when that individual requested the provision of such product, service, or service feature by subscribing to, creating an account, or otherwise contracting with a covered entity; (ii) initiation, management, execution, or completion of a financial or commercial transaction or fulfill an order for specific products or services requested by an individual, including any associated routine administrative, operational, and account-servicing activity such as billing, shipping, delivery, storage, and accounting; (iii) compliance with an obligation under federal or state law; or (iv) response to an emergency service agency, an emergency alert, a 911 communication, or any other communication reporting an imminent threat to human life.

(13) “Process”, to perform any action or set of actions on or with location information, including but not limited to collecting, accessing, using, storing, retaining, analyzing, creating, generating, aggregating, altering, correlating, operating on, recording, modifying, organizing, structuring, disposing of, destroying, de-identifying, or otherwise manipulating location information. This term does not include disclosing location information.

(14) “Reasonably understandable”, of length and complexity such that an individual with an eighth-grade reading level, as established by the department of elementary and secondary education, can read and comprehend.

(15) “Service feature”, a discrete aspect of a service provided by a covered entity, including but not limited to real-time directions, real-time weather, and identity authentication.

(16) "Service provider”, an individual, partnership, corporation, limited liability company, association, or other group, however organized, that collects, processes, or transfers location information for the sole purpose of, and only to the extent that such service provider is, conducting business activities on behalf of, for the benefit of, at the direction of, and under contractual agreement with a covered entity.

(17) “Third party”, any covered entity or person other than (i) a covered entity that collected or processed location information in accordance with this chapter or its service providers, or (ii) the individual to whom the location information pertains. This term does not include government entities.

Section 2. Protection of location information

(a) It shall be unlawful for a covered entity to collect or process an individual’s location information except for a permissible purpose. Prior to collecting or processing an individual’s location information for one of those permissible purposes, a covered entity shall provide the individual with a copy of the Location Privacy Policy and obtain consent from that individual; provided, however, that this shall not be required when the collection and processing is done in (1) compliance with an obligation under federal or state law or (2) in response to an emergency

service agency, an emergency alert, a 911 communication, or any other communication reporting an imminent threat to human life.

(b) If a covered entity collects location information for the provision of multiple permissible purposes, it shall be mentioned in the Location Privacy Policy and individuals shall provide discrete consent for each purpose; provided, however, that this shall not be required for the purpose of collecting and processing location information to comply with an obligation under federal or state law or to respond to an emergency service agency, an emergency alert, a 911 communication, or any other communication reporting an imminent threat to human life.

(c) A covered entity that directly delivers targeted advertisements as part of its product or services shall provide individuals with a clear, conspicuous, and simple means to opt out of the processing of their location information for purposes of selecting and delivering targeted advertisements.

(d) Consent provided under this section shall expire (1) after one year, (2) when the initial purpose for processing the information has been satisfied, or (3) when the individual revokes consent, whichever occurs first, provided that consent may be renewed pursuant to the same procedures. Upon expiration of consent, any location information possessed by a covered entity shall be permanently destroyed.

(e) It shall be unlawful for a covered entity or service provider that lawfully collects and processes location information to:

(1) collect more precise location information than necessary to carry out the permissible purpose;

(2) retain location information longer than necessary to carry out the permissible purpose;

(3) sell, rent, trade, or lease location information to third parties; or

(4) derive or infer from location information any data that is not necessary to carry out a permissible purpose.

(5) disclose, cause to disclose, or assist with or facilitate the disclosure of an individual's location information to third parties, unless such disclosure is (i) necessary to carry out the permissible purpose for which the information was collected, or (ii) requested by the individual to whom the location data pertains.

(f) It shall be unlawful for a covered entity or service providers to disclose location information to any federal, state, or local government agency or official unless (1) the agency or official serves the covered entity or service provider with a valid warrant or establishes the existence of exigent circumstances that make it impracticable to obtain a warrant, (2) disclosure is mandated under federal or state law, including in response to a court order or lawfully issued and properly served subpoena or civil investigative demand under state or federal law, or (3) the data subject requests such disclosure.

(g) A covered entity shall maintain and make available to the data subject a Location Privacy Policy, which shall include, at a minimum, the following:

(1) the permissible purpose for which the covered entity is collecting, processing, or disclosing any location information;

(2) the type of location information collected, including the precision of the data;

(3) the identities of service providers with which the covered entity contracts with respect to location data;

(4) any disclosures of location data necessary to carry out a permissible purpose and the identities of the third parties to whom the location information could be disclosed;

(5) whether the covered entity's practices include the internal use of location information for purposes of targeted advertisement;

(6) the data management and data security policies governing location information; and

(7) the retention schedule and guidelines for permanently deleting location information.

(h) A covered entity in lawful possession of location information shall provide notice to individuals to whom that information pertains of any change to its Location Privacy Policy at least 20 business days before the change goes into effect, and shall request and obtain consent before collecting or processing location information in accordance with the new Location Privacy Policy.

(i) It shall be unlawful for a government entity to monetize location information.

Section 3: Prohibition Against Retaliation

A covered entity shall not take adverse action against an individual because the individual exercised or refused to waive any of such individual's rights under this chapter, unless location data is essential to the provision of the good, service, or service feature that the individual requests, and then only to the extent that such data is essential. This prohibition includes but is not limited to:

(1) refusing to provide a good or service to the individual;

(2) charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; or

(3) providing a different level or quality of goods or services to the individual.

Section 4. Enforcement

(a) A violation of this chapter or a regulation promulgated under this chapter regarding an individual's location information 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 chapter 93A.

(b) Any individual alleging a violation of this chapter by a covered entity or service provider may bring a civil action in the superior court or any court of competent jurisdiction; provided that, venue in the superior court shall be proper in the county in which the plaintiff resides or was located at the time of any violation.

(c) 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 arising under this chapter.

(d) In a civil action in which the plaintiff prevails, the court may award (1) actual damages, including damages for emotional distress, or $5,000 per violation, whichever is greater, (2) punitive damages; and (3) any other relief, including but not limited to an injunction or declaratory judgment, that the court deems to be appropriate. The court shall consider each instance in which a covered entity or service provider collects, processes, or discloses location information in a manner prohibited by this chapter or a regulation promulgated under this chapter

as constituting a separate violation of this chapter or regulation promulgated under this chapter. In addition to any relief awarded, the court shall award reasonable attorney's fees and costs to any prevailing plaintiff.

(e) The attorney general may bring an action pursuant to section 4 of chapter 93A against a covered entity or service provider to remedy violations of this chapter and for other relief that may be appropriate.

(f) 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 Location 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.

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

Section 5. Implementation

The Attorney General may adopt, amend or repeal rules and regulations for the implementation, administration, and enforcement of this chapter.

SECTION 3. Location Information Collected Before Effective Date

Location information collected, processed, and stored prior to the effective date of this Act shall be subject to subsections 2(e)(3), 2(e)(5), and 2(f) of Chapter 93N.

SECTION 4. The first data protection assessments required by section 8 shall be completed not later than one year from the effective date of this Act.

SECTION 5. Section 1 shall take effect one year after enactment.

SECTION 6. Sections 2 and 3 shall take effect six months after enactment.