HOUSE . . . . . No. 4632

The Commonwealth of Massachusetts

HOUSE OF REPRESENTATIVES, May 13, 2024.

The committee on Advanced Information Technology, the Internet and Cybersecurity, to whom were referred the petition (accompanied by bill, Senate, No. 227) of Barry R. Finegold for legislation to establish the Massachusetts Information Privacy and Security Act; the petition (accompanied by bill, House, No. 60) of Daniel R. Carey and Mindy Domb relative to the security and the protection of personal information by establishing the Massachusetts information privacy and security act; the petition (accompanied by bill, House, No. 63) of Dylan A. Fernandes, Mindy Domb and Bud L. Williams for legislation to protect biometric information; the petition (accompanied by bill, House, No. 80) of David M. Rogers relative to internet privacy rights for children; and, the petition (accompanied by bill, House, No. 83) of Andres X. Vargas, David M. Rogers and Carmine Lawrence Gentile for legislation to establish the Massachusetts data privacy protection act, reports recommending that the accompanying bill (House, No. 4632) ought to pass.

For the committee,

TRICIA FARLEY-BOUVIER.

FILED ON: 5/6/2024

HOUSE . . . . . No. 4632

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Third General Court
(2023-2024)

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, the following words shall, unless the context clearly requires otherwise, have the following meanings:

(1) “authentication”, the process of verifying an individual or entity for security purposes.

(2) “biometric data”, data generated from the technological processing of an individual’s unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual, including but not limited to retina or iris scans, fingerprint,

voiceprint, map or scan of hand or face geometry, vein pattern, gait pattern; provided, however, that “biometric information” shall not include:

(i) a digital or physical photograph;

(ii) an audio or video recording; or

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

(3) "chapter”, this chapter of the General Laws, as from time to time may be amended, and any regulations promulgated under said chapter.

(4) “collect” and “collection”, buying, renting, licensing, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means. This includes receiving information from the consumer either actively, through interactions such as user registration, or passively, by observing the consumer’s behavior.

(5) “consent”, a clear affirmative act signifying an individual’s freely given, specific, informed, and unambiguous agreement to allow the processing of specific categories of personal information relating to the individual for a narrowly defined particular purpose after having been informed, in response to a specific request from a covered entity that meets the requirements of this chapter; provided, however, that “consent” may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action; and provided further, that the following shall not constitute “consent”:

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

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

(iii) agreement obtained through dark patterns or a false, fictitious, fraudulent, or materially misleading statement or representation.

(6) "control", with respect to an entity:

(i) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of the entity;

(ii) control over the election of a majority of the directors of the entity (or of individuals exercising similar functions); or

(iii) the power to exercise a controlling influence over the management of the entity.

(7) "covered data", information, including derived data, inferences, and unique persistent identifiers, that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual. However, the term "covered data" does not include de-identified data or publicly available information.

(8) "covered entity", any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data.

The term "covered entity" does not include:

(i) government agencies or service providers to government agencies that exclusively and solely process information provided by government entities;

(ii) any entity or person that meets the following criteria for the period of the 3 preceding calendar years (or for the period during which the covered entity or service provider has been in existence if such period is less than 3 years):

(A) the entity or person's average annual gross revenues during the period did not exceed $20,000,000;

(B) the entity or person, on average, did not annually collect or process the covered data of more than 25,000 individuals during the period, other than for the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product, so long as all covered data for such purpose was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a covered entity's return policy; and

(C) no component of its revenue comes from transferring covered data during any year (or part of a year if the covered entity has been in existence for less than 1 year) that occurs during the period.

(iii) a national securities association that is registered under 15 U.S.C. 78o-3 of the Securities Exchange Act of 1934.and is operating solely for purposes under that act.

(iv) a nonprofit organization that is established to detect and prevent fraudulent acts in connection with insurance and is operating solely for that purpose.

(9) "covered high-impact social media company", a covered entity that provides any internet-accessible platform where:

(i) such covered entity generates $3,000,000,000 or more in annual revenue;

(ii) such platform has 300,000,000 or more monthly active users for not fewer than 3 of the preceding 12 months on the online product or service of such covered entity; and

(iii) such platform constitutes an online product or service that is primarily used by users to access or share user-generated content.

(10) "dark pattern or deceptive design", a user interface that is designed, modified, or manipulated with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision-making, or choice, including, but not limited to, any practice the Federal Trade Commission refers to as a "dark pattern."

(11) "data broker", a covered entity whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to the covered data. This term does not include a covered entity insofar as such entity processes employee data collected by and received from a third party concerning any individual who is an employee of the third party for the sole purpose of such third-party providing benefits to the employee. An entity may not be considered to be a data broker for purposes of this chapter if the entity is acting as a service provider.

(12) "de-identified data", information that does not identify and is not linked or reasonably linkable to a distinct individual or a device, regardless of whether the information is aggregated, and if the covered entity or service provider:

(i) takes technical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual;

(ii) publicly commits in a clear and conspicuous manner:

(A) to process and transfer the information solely in a de-identified form without any reasonable means for re-identification; and

(B) to not attempt to re-identify the information with any individual or device that identifies or is linked or reasonably linkable to an individual; and

(iii) contractually obligates any person or entity that receives the information from the covered entity or service provider:

(A) to comply with all the provisions of this paragraph with respect to the information; and

(B) to require that such contractual obligations be included contractually in all subsequent instances for which the data may be received.

(13) "derived data", covered 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.

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

(15) "genetic information", any covered 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).

(16) “homepage”, the introductory page of an internet website and any internet web page where personal information is collected; provided, however, that in the case of an online service, such as a mobile application, “homepage” shall include:

(i) the application’s platform page or download page;

(ii) a link within the application, such as from the application configuration, “About,” “Information,” or settings page; and

(iii) any other location that allows individuals to review the notices required by this chapter, including, but not limited to, before downloading the application.

(17) “individual”, a natural person who is a Massachusetts resident or is present in Massachusetts.

(18) “knowledge”,

(i)with respect to a covered entity that is a covered high-impact social media company, the entity knew or should have known the individual was a minor;

(ii)with respect to a covered entity or service provider that is a large data holder, and otherwise is not a covered high-impact social media company, that the covered entity knew or acted in willful disregard of the fact that the individual was a minor; and

(iii)with respect to a covered entity or service provider that does not meet the requirements of clause (i) or (ii), actual knowledge.

(19) “large data holder”, a covered entity or service provider 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 covered data of more than 2,000,000 individuals or devices that identify or are linked or reasonably linkable to one or more individuals, excluding covered 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 covered 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 covered entity or service provider 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 covered entity or service provider.

(20) “material”, with respect to an act, practice, or representation of a covered entity (including a representation made by the covered entity in a privacy policy or similar disclosure to individuals) involving the collection, processing, or transfer of covered data, that such act, practice, or representation is likely to affect a reasonable individual’s decision or conduct regarding a product or service

(21) “minor”, an individual under the age of 18.

(22) “OCABR”, the Office of Consumer Affairs and Business Regulation.

(23) “precise geolocation information,” information derived from 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.

(24) “process”, any operation or set of operations performed on information or on sets of information, whether or not by automated means, including but not limited to the use, storage, analysis, deletion, or modification of information.

(25) “processing purpose”, a reason for which a covered entity or service provider collects, processes, or transfers covered data that is specific and granular enough for a reasonable individual to understand the material facts of how and why the covered entity or service provider collects, processes, or transfers the covered data.

(26) "profiling", any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

(27) “publicly available information”, any information that a covered entity or service provider has a reasonable basis to believe has been lawfully made available to the general public from:

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

(ii) widely distributed media;

(iii) a website or online service made available to all members of the public, for free or for a fee, including where all members of the public, for free or for a fee, can log in to the website or online service;

(iv) a disclosure that has been made to the general public as required by federal, state, or local law; or

(v) the visual observation of the physical presence of an individual or a device in a public place, not including data collected by a device in the individual's possession.

For purposes of this paragraph, information from a website or online service is not available to all members of the public if the individual who made the information available via the website or online service has either restricted the information to a specific audience or reasonably expects that the information will not be distributed to so many persons as to become a matter of public knowledge.

The term "publicly available information" does not include:

(i) any obscene visual depiction, as defined in 18 U.S.C. section 1460;

(ii) any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive covered data with respect to an individual;

(iii) biometric information;

(iv) publicly available information that has been combined with covered data;

(v) genetic information, unless otherwise made available by the individual to whom the information pertains:

(vi) intimate images known to have been created or shared without consent.

(28) “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.

(29) “sensitive covered data”, a form of coved data, including:

(i) an individual’s precise geolocation information;

(ii) biometric or genetic information;

(iii) the covered data of an individual when a covered entity or service provider has knowledge the individual is a minor;

(iv) covered data that reveals an individual’s:

(A) race, color, ethnicity, or national origin;

(B) sex or gender identity;

(C) religious beliefs;

(D) citizenship or immigration status;

(E) military service; or

(F) status as a victim of a crime.

(v) covered data processed concerning an individual's past, present or future mental or physical health condition, disability, diagnosis or treatment, including pregnancy and cosmetic treatment;

(vi) covered data processed concerning an individual's sexual orientation, sex life or reproductive health, including, but not limited to, the use or purchase of contraceptives, birth control, abortifacients or other medication, products or services related to reproductive health;

(vii) covered data that reveals an individual's philosophical beliefs or union membership;

(viii) covered data that reveals an individual's government-issued identifier, including but not limited to, social security number, driver's license number, military identification number, passport number or state-issued identification card number but does not include a government-issued identifier required by law to be displayed in public;

(ix) covered data that reveals an individual's financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account, or information that describes or reveals the income level or bank account balances of an individual;

(x) covered data that reveals account or device log-in credentials, or security or access codes for an account or device;

(xi) covered data that reveals an individual's private communications such as voicemails, emails, texts, direct messages, or mail, or information identifying the parties to such communications, voice communications, video communications, and any information that pertains 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, unless the covered entity or a service provider acting on behalf of the covered entity is the sender or an intended recipient of the communication. Communications are not private for purposes of this clause 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;

(xii) covered data that reveals 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 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.

(xiii) a photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual;

(xiv) covered data that reveals the video content requested or selected by an individual collected by a covered entity. This clause does not include covered data used solely for transfers for independent video measurement.

(xv) covered data that reveals an individual's online activities over time and across third-party websites or online services.

(xvi) any other covered data collected, processed, or transferred for the purpose of identifying the types of covered data listed in clauses (i) through (xv), inclusive.

(30) "service provider", a person or entity that:

(i) collects, processes, or transfers covered data on behalf of, and at the direction of, a covered entity or a government agency; and

(ii) receives covered data from or on behalf of a covered entity or a government agency.

A service provider that receives service provider data from another service provider as permitted under this chapter shall be treated as a service provider under this chapter with respect to such data.

(31) "service provider data", covered data that is collected or processed by or has been transferred to a service provider by or on behalf of a covered entity or a government agency or another service provider for the purpose of allowing the service provider to whom such covered data is transferred to perform a service or function on behalf of, and at the direction of, such covered entity or government agency.

(32) “targeted advertising”, presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics, or interests associated with the individual or a device identified by a unique identifier; provided, however, that “targeted advertising” does not include:

(i) advertising or marketing to an individual or an individual’s device in response to the individual’s specific request for information or feedback;

(ii) contextual advertising, which is when an advertisement is displayed based on the content with or in which the advertisement appears and does not vary based on who is viewing the advertisement; or

(iii) processing covered data strictly necessary for the sole purpose of measuring or reporting advertising or content performance, reach, or frequency, including independent measurement.

(33) “third party”, any person or entity, including a covered entity, that

(i) collects, processes, or transfers covered data and is not a consumer-facing business with which the individual linked or reasonably linkable to such covered data expects and intends to interact; and

(ii) is not a service provider with respect to such data.

This term does not include a person or entity that collects covered data from another entity if the two entities are related by common ownership or corporate control, but only if a reasonable consumer’s reasonable expectation would be that such entities share information.

(34) “third party data”, covered data that has been transferred to a third party.

(35) “transfer”, to disclose, sell, release, disseminate, make available, license, rent, or share covered data orally, in writing, electronically, or by any other means.

(36) “unique identifier”, an identifier to the extent that such identifier is reasonably linkable to an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals, including a device identifier, Internet Protocol address, cookie, beacon, pixel tag, mobile ad identifier, or similar technology, customer number, unique pseudonym, user alias, telephone number, or other form of persistent or probabilistic identifier that is linked or reasonably linkable to an individual or device. This term does not include an identifier assigned by a covered entity for the specific purpose of giving effect to an individual’s exercise of consent or opt-outs of the collection, processing, and transfer of covered data pursuant to this chapter or otherwise limiting the collection, processing, or transfer of such information.

(37) “widely distributed media”, information that is available to the general public, including information from a telephone book or online directory, a television, internet, or radio program, the news media, or an internet site that is available to the general public on an unrestricted basis, but does not include an obscene visual depiction, as defined in 18 U.S.C. section 1460.

Section 2. Duty of Loyalty

(a)A covered entity or service provider may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to carry out one of the following purposes:

(1)provide or maintain a specific product or service requested by the individual to whom the data pertains;

(2)initiate, manage, complete a 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;

(3)authenticate users of a product or service;

(4)fulfill a product or service warranty;

(5)prevent, detect, protect against, or respond to a security incident. For purposes of this paragraph, security is defined as network security and physical security and life safety, including an intrusion or trespass, medical alerts, fire alarms, and access control security;

(6)to prevent, detect, protect against, or respond to fraud, harassment, or illegal activity targeted at or involving the covered entity or its services. For purposes of this paragraph, the term “illegal activity”, a violation of a federal, state, or local law punishable as a felony or misdemeanor that can directly harm;

(7)comply with a legal obligation imposed by state or federal law, or to investigate, establish, prepare for, exercise, or defend legal claims involving the covered entity or service provider;

(8)effectuate a product recall pursuant to state or federal law;

(9)conduct a public or peer-reviewed scientific, historical, or statistical research project that:

(i)is in the public interest; and

(ii)adheres to all relevant laws and regulations governing such research, including regulations for the protection of human subjects, or is excluded from criteria of the institutional review board;

(10)deliver a communication that is not an advertisement to an individual, if the communication is reasonably anticipated by the individual within the context of the individual's interactions with the covered entity;

(11)deliver a communication at the direction of an individual between such individual and one or more individuals or entities;

(12)ensure the data security and integrity of covered data in accordance with chapter 93H; or

(13)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 covered entity's assets, only if the covered entity, in a reasonable time prior to such transfer, provides each affected individual with:

(i)a notice describing such transfer, including the name of the entity or entities receiving the individual's covered data and their privacy policies; and

(ii)a reasonable opportunity to withdraw any previously given consents related to the individual's covered data and a reasonable opportunity to request the deletion of the individual's covered data.

(b)A covered entity or service provider may, with respect to covered data previously collected in accordance with the previous subsection, process such data:

(1) as necessary to provide advertising or marketing of products or services provided by the covered entity to an individual who is not a minor or device by electronic or non-electronic means, provided that the delivery of such advertising or marketing complies with the requirements of this chapter;

(2)process such data as necessary to perform system maintenance or diagnostics;

(3)develop, maintain, repair, or enhance a product or service for which such data was collected;

(4)to conduct internal research or analytics to improve a product or service for which such data was collected;

(5)perform inventory management or reasonable network management;

(6)protect against spam; or

(7)debug or repair errors that impair the functionality of a service or product for which such data was collected.

(c)A covered entity or service provider shall not:

(1) engage in deceptive advertising or marketing with respect to a product or service offered to an individual; or

(2)draw an individual into signing up for or acquiring a product or service through:—

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

(ii)the use of a dark pattern or deceptive design.

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

(1)limit or diminish free speech rights of covered entities guaranteed under the First Amendment to the Constitution of the United States or under Article 16 of Massachusetts Declaration of Rights; or

(2)imply any purpose that is not enumerated in subsections (a) and (b), when applicable.

Section 3. Sensitive Covered Data

(a)A covered entity or service provider shall not:

(1)collect, process, or transfer a Social Security number, except when necessary to facilitate an extension of credit, authentication, fraud and identity fraud detection and prevention, the payment or collection of taxes, the enforcement of a contract between parties, or the prevention, investigation, or prosecution of fraud or illegal activity, or as otherwise required by state or federal law;

(2)collect or process sensitive covered data, except where such collection or processing is strictly necessary to provide or maintain a specific product or service requested by the individual to whom the covered data pertains or is strictly necessary to effect a purpose enumerated in paragraphs (1), (2), (3), (5), (7), (9), (10), (11), (13), of subsection (a) of section 2, and such data is only used for that purposes;

(3)transfer an individual's sensitive covered data to a third party, unless:

(i)the transfer is made pursuant to the consent of the individual, given before each specific transfer takes place;

(ii)the transfer is necessary to comply with a legal obligation imposed by state or federal law, so long as such obligation preexisted the collection and previous notice of such obligation was provided to the individual to whom the data pertains;

(iii)the transfer is necessary to prevent an individual from imminent injury where the covered entity believes in good faith that the individual is at risk of death, serious physical injury, or serious health risk;

(iv)in the case of the transfer of a password, the transfer is necessary to use a designated password manager or is to a covered entity for the exclusive purpose of identifying passwords that are being reused across sites or accounts;

(v)in the case of the transfer of genetic information, the transfer is necessary to perform a medical diagnosis or medical treatment specifically requested by an individual, or to conduct medical research in accordance with federal and state law; or

(vi)in the case of transfer assets in case of a merger, if the transfer is made in accordance with paragraph (13) of subsection (a) of section (2); or

(4)process sensitive covered data for the purposes of targeted advertising.

Section 4. Data Subject Rights

(a)A covered entity shall provide an individual, after receiving a verified request from the individual, with the right to:

(1)access:

(i)in a human-readable format that a reasonable individual can understand and download from the internet and transmit freely, the covered data (except covered data in a back-up or archival system) of the individual making the request that is collected, processed, or transferred by the covered entity or any service provider of the covered entity within the 12 months preceding the request;

(ii)the categories of any third party or service provider, if applicable, and an option for consumers to obtain the names of any such third party as well as and the categories of any service providers to whom the covered entity has transferred the covered data of the individual, as well as the categories of sources from which the covered data was collected; and

(iii)a description of the purpose for which the covered entity transferred the covered data of the individual to a third party or service provider;

(2)correct any verifiable substantial inaccuracy or substantially incomplete information with respect to the covered data of the individual that is processed by the covered entity and instruct the covered entity to make reasonable efforts to notify all third parties or service providers to which the covered entity transferred such covered data of the corrected information;

(3)delete covered data of the individual that is processed by the covered entity and instruct the covered entity to make reasonable efforts to notify all third parties or service

provider to which the covered entity transferred such covered data of the individual's deletion request; and

(4)to the extent technically feasible, export to the individual or directly to another entity the covered data of the individual that is processed by the covered entity, including inferences linked or reasonably linkable to the individual but not including other derived data, without licensing restrictions that limit such transfers in:

(i)a human-readable format that a reasonable individual can understand and download from the internet and transmit freely; and

(ii)a portable, structured, interoperable, and machine-readable format.

(b)A covered entity may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a right described in subsection (a) through:

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

(2) the use of any dark pattern or deceptive design.

(c)Subject to subsections (d) and (e), each request under subsection (a) shall be completed within 45 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual's request.

(d)A response period set forth in this subsection may be extended once by 20 additional days when reasonably necessary, considering the complexity and number of the individual's requests, so long as the covered entity informs the individual of any such extension within the initial 45-day response period, together with the reason for the extension.

(e)A covered entity:

(1)shall provide an individual with the opportunity to exercise each of the rights described in subsection (a) and with respect to:

(i)the first two times that an individual exercises any right described in subsection (a) in any 12-month period, shall allow the individual to exercise such right free of charge; and

(ii)any time beyond the initial two times described in subparagraph (i), may allow the individual to exercise such right for a reasonable fee for each request.

(f)A covered entity may not permit an individual to exercise a right described in subsection (a), in whole or in part, if the covered entity:

(1)cannot reasonably verify that the individual making the request to exercise the right is the individual whose covered data is the subject of the request or an agent authorized to make such a request on the individual's behalf;

(2)reasonably believes that the request is made to interfere with a contract between the covered entity and another individual;

(3)determines that the exercise of the right would require access to or correction of another individual's sensitive covered data;

(4)reasonably believes that the exercise of the right would require the covered entity to engage in an unfair or deceptive practice under state law; or

(5)reasonably believes that the request is made to further fraud, support criminal activity, or the exercise of the right presents a data security threat.

(g)If a covered entity cannot reasonably verify that a request to exercise a right described in subsection (a) is made by the individual whose covered data is the subject of the request, the covered entity:

(1)may request that the individual making the request to exercise the right provide any additional information necessary for the sole purpose of verifying the identity of the individual; and

(2)may not process or transfer such additional information for any other purpose.

(h)A covered entity may decline, with adequate explanation to the individual, to comply with a request to exercise a right described in subsection (a), in whole or in part, that would:

(1)require the covered entity to retain any covered data collected for a single, one-time transaction, if such covered data is not processed or transferred by the covered entity for any purpose other than completing such transaction;

(2)be demonstrably impracticable or prohibitively costly to comply with, and the covered entity shall provide a description to the requestor detailing the inability to comply with the request;

(3)require the covered entity to attempt to re-identify any de-identified data;

(4)require the covered entity to either maintain covered data in an identifiable form or to collect, retain, or access any data in order to be capable of associating a verified individual request with covered data of such individual;

(5)result in the release of trade secrets or other privileged or confidential business information;

(6)require the covered entity to correct any covered data that cannot be reasonably verified as being inaccurate or incomplete;

(7)interfere with law enforcement, judicial proceedings, investigations, or reasonable efforts to guard against, detect, prevent, or investigate fraudulent, malicious, or unlawful activity, or enforce valid contracts;

(8)violate state or federal law or the rights and freedoms of another individual, including under the Constitution of the United States and Massachusetts Declaration of Rights;

(9)prevent a covered entity from being able to maintain a confidential record of deletion requests, maintained solely for the purpose of preventing covered data of an individual from being recollected after the individual submitted a deletion request and requested that the covered entity no longer collect, process, or transfer such data; or

(10)endanger the source of the data if such data could only have been obtained from a single identified source.

(i)A covered entity may decline, with adequate explanation to the individual, to comply with a request for deletion pursuant to paragraph (3) of subsection (a) if such request:

(1)unreasonably interferes with the provision of products or services by the covered entity to another person it currently serves;

(2)requests to delete covered data that relates to (A) a public figure, public official, or limited-purpose public figure; or (B) any other individual that has no reasonable expectation of privacy with respect to such data;

(3)requests to delete covered data reasonably necessary to perform a contract between the covered entity and the individual;

(4)requests to delete covered data that the covered entity needs to retain in order to comply with professional ethical obligations;

(5)requests to delete covered data that the covered entity reasonably believes may be evidence of unlawful activity or an abuse of the covered entity's products or service; or

(6) is directed to a consumer reporting agency, as defined in 15 U.S.C. 1681a(f) and targets covered data that is 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 and strictly maintained in accordance with, the provisions of the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.

(j)In a circumstance that would allow a denial pursuant to this section, a covered entity shall partially comply with the remainder of the request if it is possible and not unduly burdensome to do so.

(k)The receipt of a large number of verified requests, on its own, may not be considered to render compliance with a request demonstrably impracticable.

(l)A covered entity shall facilitate the ability of individuals to make requests under subsection (a) in any language in which the covered entity provides a product or service. The mechanisms by which a covered entity enables individuals to make requests under subsection (a) shall be readily accessible and usable by individuals with disabilities. Such mechanisms shall, at

a minimum, be accessible in the same or a similar location as the privacy policies required by section 9 of this chapter.

Section 5. Consent Practices

(a)The requirements of this chapter with respect to a request for consent from a covered entity or service provider to an individual are the following:

(1)The request for consent shall be provided to the individual in a clear and conspicuous standalone disclosure made through the primary medium used to offer the covered entity's product or service, or, in the case that the product or service is not offered in a medium that does permits the making of the request under this paragraph, another medium regularly used in conjunction with the covered entity's product or service;

(2)The request includes a description of the processing purpose for which the individual's consent is sought by:

(i)clearly stating the specific categories of covered data that the covered entity shall collect, process, and transfer necessary to effectuate the processing purpose; and

(ii)including a prominent heading and is reasonably understandable so that an individual can identify and understand the processing purpose for which consent is sought and the covered data to be collected, processed, or transferred by the covered entity for such processing purpose;

(3)The request clearly explains the individual's applicable rights related to consent;

(4)The request is made in a manner reasonably accessible to and usable by individuals with disabilities;

(5)The request is made available to the individual in each covered language in which the covered entity provides a product or service for which authorization is sought;

(6)The option to refuse consent shall be at least as prominent as the option to accept, and the option to refuse consent shall take the same number of steps or fewer as the option to accept;

(7)Processing or transferring any covered data collected pursuant to consent for a different processing purpose than that for which consent was obtained shall require consent for the subsequent processing purpose;

(8)The request for consent must be displayed at or before the point of collection; and

(9) The request must be accompanied by a copy of the covered entity's or service provider's privacy policy subject to the requirements of section 9, which may be included with the request as a hyperlink, and, if the covered entity is a large data holder, shall also include the short form privacy policy as required by subsection (h) of section 9.

(b)A covered entity shall not infer that an individual has provided consent to a practice from the inaction of the individual or the individual's continued use of a service or product provided by the covered entity.

(c)A covered entity shall not obtain or attempt to obtain the consent of an individual through:

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

(2) the use of any dark pattern or deceptive design; or

(3) conditioning or limiting access to an individual's account.

Section 6. Privacy by Design

(a)A covered entity or service provider shall establish, implement, and maintain reasonable policies, practices, and procedures that reflect the role of the covered entity or service provider in the collection, processing, and transferring of covered data and that:

(1)consider applicable federal and state laws, rules, or regulations related to covered data the covered entity or service provider 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 covered entity or the service provider, including in the design, development, and implementation of such products and services, considering the role of the covered entity or service provider and the information available to it;

(4)evaluate the length of time that covered data shall be retained and circumstances under which covered 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 covered data; and

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

(b)The policies, practices, and procedures established by a covered entity or service provider under subsection (a), shall correspond with, as applicable:

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

(2)the sensitivity of the covered data collected, processed, or transferred by the covered entity or service provider;

(3)the volume of covered data collected, processed, or transferred by the covered entity or service provider;

(4)the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity or service provider relates; and

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

Section 7. Pricing

(a) A covered entity may not retaliate against an individual for:

(1)exercising any of the rights guaranteed by this chapter, or any regulations promulgated under this chapter; or

(2)refusing to agree to collection or processing of covered 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.

(b) Nothing in subsection (a) shall be construed to:

(1)prohibit the relation of the price of a service or the level of service provided to an individual to the provision, by the individual, of financial information that is necessarily collected and processed only for the purpose of initiating, rendering, billing for, or collecting payment for a service or product requested by the individual;

(2)prohibit a covered entity from offering a different price, rate, level, quality or selection of goods or services to an individual, including offering goods or services for no fee, if the offering is in connection with an individual's voluntary participation in a bona fide loyalty, rewards, premium features, discount or club card program, provided, that the covered entity may not sell covered data to a third-party as part of such a program unless:

(i)the sale is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled;

(ii)the sale of personal data to third parties is clearly disclosed in the terms of the program; and

(iii)the third party uses the personal data only for purposes of facilitating such a benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose;

(3)require a covered entity to provide a bona fide loyalty program that would require the covered entity to collect, process, or transfer covered data that the covered entity otherwise would not collect, process, or transfer;

(4)prohibit a covered entity from offering a financial incentive or other consideration to an individual for participation in market research;

(5)prohibit a covered entity from offering different types of pricing or functionalities with respect to a product or service based on an individual's exercise of a right to delete; or

(6)prohibit a covered entity from declining to provide a product or service insofar as the collection and processing of covered data is strictly necessary for such product or service.

(c) Notwithstanding the provisions in this section, no covered entity may offer different types of pricing that are unjust, unreasonable, coercive, or usurious in nature.

Section 8. Civil Rights Protections

(a) A covered entity or a service provider may not collect, process, or transfer covered data or publicly available data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services (i.e., has a disparate impact) on the basis of race, color, religion, national origin, sex, sexual orientation, gender identity, disability, genetic information, pregnancy or a condition related to said pregnancy including, but not limited to, lactation or the need to express breast milk for a nursing child, ancestry or status as a veteran, or any other basis protected by chapter 151B.

(b) This subsection shall not apply to:

(1) the collection, processing, or transfer of covered data for the purpose of:

(i) covered entity's or a service provider's self-testing to prevent or mitigate unlawful discrimination; or

(ii) diversifying an applicant, participant, or customer pool; or

(2) any private club or group not open to the public, as described in section 201(e) of the Civil Rights Act of 1964, 42 U.S.C. section 2000a(e).

(c) Whenever the Attorney General obtains information that a covered entity or service provider may have collected, processed, or transferred covered data in violation of subsection (a), the Attorney General shall initiate enforcement actions relating to such violation in accordance with section 12 of this chapter.

(1) Not later than 3 years after the date of enactment of this chapter, and annually no later than December 31 of each year thereafter, the Attorney General shall submit to the joint committee on ways and means, the joint committee on racial equity, civil rights, and inclusion, and the joint committee on advanced information technology, the internet and cybersecurity a report that includes a summary of the enforcement actions taken under this subsection.

Section 9. Privacy Policy

(a)Each covered entity or service provider shall make publicly available, in a clear and conspicuous location on its homepage, a reasonably understandable and not misleading privacy policy that provides a detailed and accurate representation of the data collection, processing, and transfer activities of the covered entity or service provider.

(b)The privacy policy must be provided in a manner that is reasonably accessible to and usable by individuals with disabilities. The policy shall be made available to the public in each

covered language in which the covered entity or service provider provides a product or service that is subject to the privacy policy; or carries out activities related to such product or service.

(c)The privacy policy must include, at a minimum:

(1)The identity and the contact information of:

(i)the covered entity or service provider to which the privacy policy applies, including the covered entity's or service provider's points of contact and generic electronic mail addresses, as applicable for privacy and data security inquiries;

(ii)any other entity within the same corporate structure as the covered entity or service provider to which covered data is transferred by the covered entity;

(2)the categories of covered data the covered entity or service provider collects or processes;

(3)the processing purposes for each category of covered data the covered entity or service provider collects or processes;

(4)whether the covered entity or service provider transfers covered data and, if so, each category of service provider and third party to which the covered entity or service provider transfers covered data, the name of each data broker to which the covered entity or service provider transfers covered data, and the purposes for which such data is transferred to such categories of service providers and third parties or third-party collecting entities, except for a transfer to a governmental entity pursuant to a court order or law that prohibits the covered entity or service provider from disclosing such transfer;

(5)The length of time the covered entity or service provider intends to retain each category of covered data, including sensitive covered data, or, if it is not possible to identify that timeframe, the criteria used to determine the length of time the covered entity or service provider intends to retain categories of covered data;

(6)A prominent, clear, and reasonably understandable description of how an individual can exercise the rights described in this chapter;

(7)A general description of the covered entity's or service provider's data security practices; and

(8)The effective date of the privacy policy.

(d)If a covered entity or service provider makes a material change to its privacy policy or practices, the covered entity or service provider shall notify each individual affected by such material change before implementing the material change with respect to any prospectively collected covered data and, except as provided in paragraphs (1) through (13) of section 2, subsection (a), provide a reasonable opportunity for each individual to withdraw consent to any further materially different collection, processing, or transfer of previously collected covered data under the changed policy.

(e)A covered entity or service provider shall take all reasonable electronic measures to provide direct notification regarding material changes to the privacy policy to each affected individual, in each covered language in which the privacy policy is made available, and taking into account available technology and the nature of the relationship.

(f)Nothing in this section shall be construed to affect the requirements for covered entities or service providers under other sections of this chapter.

(g)Each large data holder shall retain copies of previous versions of its privacy policy 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 policy 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 policy, or any material changes to such policy, that precede the date of enactment of this Act.

(h)In addition to the privacy policy required under subsection (a), a large data holder that is a covered entity shall provide a short form notice of no more than 500 words in length that includes the main features of their data practices.

(i)Each covered entity or service provider that collects, processes, or transfers biometric data shall provide a separate privacy policy detailing the collection, processing, and transfer of such biometric data, subject to the provisions of subsections (a) through (h) of this section.

(j)Each covered entity or service provider that collects, processes, or transfers specific precise geolocation information shall provide a separate privacy policy detailing the collection, processing, and transfer of such precise geolocation information, subject to the provisions of subsections (a) through (h) of this section.

Section 10. Advanced Data Rights

(a) A covered entity or service provider shall provide an individual with a clear and conspicuous, easy-to-execute means to withdraw consent. Those means shall be at least as easy to execute by an individual as the means to provide consent and shall, at a minimum, be accessible in the same or a substantially similar location as the privacy policies required by section 9.

(b) Right to opt out of covered data transfers. A covered entity:

(1) may not transfer or direct the transfer of the covered data of an individual to a third party if the individual or an agent authorized to make such a request on the individual's behalf objects to the transfer; and

(2) shall allow an individual to object to such a transfer through an opt out mechanism, at a minimum, accessible in the same or a substantially similar location as the privacy policies required by section 9.

(c) Right to opt out of targeted advertising. A covered entity or service provider that directly delivers a targeted advertisement shall:

(1) prior to engaging in targeted advertising to an individual or device and at all times, thereafter, provide such individual with a clear and conspicuous means to opt out of targeted advertising;

(2) abide by any opt out designation by an individual or an agent authorized to make such a request on the individual's behalf with respect to targeted advertising and notify the covered entity that directed the service provider to deliver the targeted advertisement of the opt out decision; and

(3) allow an individual to make an opt out designation with respect to targeted advertising through an opt out mechanism, at a minimum, accessible in the same or a substantially similar location as the privacy policies required by section 9.

(d) Right to opt out of profiling. A covered entity or service provider that engages in profiling in furtherance of automated decisions that produce legal or similarly significant effects on an individual shall:

(1) provide such individual with a clear and conspicuous means to opt out of such profiling; and

(2) allow an individual to object to such profiling through an opt out mechanism, at a minimum, accessible in the same or a substantially similar location as the privacy policies required by section 9.

(e) A covered entity or service provider that receives an opt out notification pursuant to this section shall abide by such opt out designations in a commercially reasonable timeframe. Such covered entity or service provider shall notify any other person that directed the covered entity or service provider to either serve, deliver, or otherwise process targeted advertisements or to engage in profiling in furtherance of automated decisions of the individual's opt out decision within a commercially reasonable timeframe.

(f) A covered entity or service provider may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of any individual right under this section through:

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

(2) the use of a dark pattern or deceptive design.

(g) A covered entity shall notify third parties who had access to an individual's covered data when the individual exercises any of the rights established in this section. The third party shall comply with the request to opt out of sale or data transfer forwarded to them from a covered entity that provided, made available, or authorized the collection of the individual's covered data. The third party shall comply with the request in the same way a covered entity is required to comply with the request. The third party shall no longer retain, use, or disclose the personal information unless the third party becomes a service provider or a covered entity in the terms of this chapter.

(h) A covered entity that communicates an individual's opt out request to a third party or service provider pursuant to this section shall not be liable under this chapter if the third party or service provider receiving the opt-out request violates the restrictions set forth in this chapter; provided, however, that at the time of communicating the opt-out request, the covered entity does not know or should not reasonably know that the third party or service provider intends to commit such a violation.

(i) If an individual decides to opt out of the processing of the individual's covered data for the purposes specified in subsections (b), (c), or (d) and such decision conflicts with the individual's existing, voluntary participation in a covered entity's bona fide loyalty, rewards, premium features, discounts or club card program, the covered entity shall comply with the individual's opt out preference signal but may notify the individual of the conflict and provide

the individual with the choice to opt back into such processing for participation in such a program; provided, however, that the controller shall not use dark patterns or deceptive design to coerce the individual to opt back into such processing related to that individual's participation in such program.

(j) A covered entity or service provider shall not require an individual to create an account for the purposes of exercising any right under this chapter.

Section 11. Service Providers

(a)A service provider:

(1)shall adhere to the instructions of a covered entity and only collect, process, and transfer service provider data to the extent necessary and proportionate to provide a service requested by the covered entity, as set out in the contract required by subsection (b), and this paragraph does not require a service provider to collect, process, or transfer covered data if the service provider would not otherwise do so;

(2)may not collect, process, or transfer service provider data if the service provider has actual knowledge that a covered entity violated this chapter with respect to such data;

(3)shall assist a covered entity in responding to a request made by an individual under this chapter, by either:

(i)providing appropriate technical and organizational measures, considering the nature of the processing and the information reasonably available to the service provider, for the covered entity to comply with such request for service provider data; or

(ii)fulfilling a request by a covered entity to execute an individual rights request that the covered entity has determined should be complied with, by either:

(A)complying with the request pursuant to the covered entity's instructions; or

(B)providing written verification to the covered entity that it does not hold covered data related to the request, that complying with the request would be inconsistent with its legal obligations, or that the request falls within an exception under this chapter;

(4)may engage another service provider for purposes of processing service provider data on behalf of a covered entity only after providing that covered entity with notice and pursuant to a written contract that requires such other service provider to satisfy the obligations of the service provider with respect to such service provider data, including that the other service provider be treated as a service provider under this chapter;

(5)shall, upon the reasonable request of the covered entity, make available to the covered entity information necessary to demonstrate the compliance of the service provider with the requirements of this chapter, which may include making available a report of an independent assessment arranged by the service provider on terms agreed to by the service provider and the covered entity or providing information necessary to enable the covered entity to conduct and document a privacy impact assessment;

(6)shall, at the covered entity's direction, delete or return all covered data to the covered entity as requested at the end of the provision of services, unless retention of the covered data is required by law;

(7)shall develop, implement, and maintain reasonable administrative, technical, and physical safeguards that are designed to protect the security and confidentiality of covered data the service provider processes consistent with chapter 93H of the general laws; and

(8)shall allow and cooperate with reasonable assessments by the covered entity or the covered entity's designated assessor. Alternatively, the service provider may arrange for a qualified and independent assessor to conduct an assessment of the service provider'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 service provider shall provide a report of such assessment to the covered entity upon request.

(b)A person or entity may only act as a service provider pursuant to a written contract between the covered entity and the service provider, or a written contract between one service provider and a second service provider as described under paragraph (4) of subsection (a), if the contract:

(1)sets forth the data processing procedures of the service provider with respect to collection, processing, or transfer performed on behalf of the covered entity or service provider;

(2)clearly sets forth:

(i)instructions for collecting, processing, or transferring data;

(ii)the nature and purpose of collecting, processing, or transferring;

(iii)the type of data subject to collecting, processing, or transferring;

(iv)the duration of processing; and

(v)the rights and obligations of both parties, including a method by which the service provider shall notify the covered entity of material changes to its privacy practices;

(3)does not relieve a covered entity or a service provider of any requirement or liability imposed on such covered entity or service provider under this chapter; and

(4)prohibits:

(i)collecting, processing, or transferring covered data in contravention to subsection (a); and

(ii)combining service provider data with covered data which the service provider receives from or on behalf of another person or persons or collects from the interaction of the service provider with an individual, provided that such combining is not necessary to effectuate a purpose described in paragraphs (1) through (13) of section 2(a) and is otherwise permitted under the contract required by this subsection.

(c)Each service provider shall retain copies of previous contracts entered into in compliance with this subsection with each covered entity to which it provides requested products or services.

(d)The classification of a person or entity as a covered entity or as a service provider and the relationship between covered entities and service providers are regulated by the following provisions:

(1)Determining whether a person is acting as a covered entity or service provider with respect to a specific processing of covered data is a fact-based determination that depends upon the context in which such data is processed.

(2)A person or entity that is not limited in its processing of covered data pursuant to the instructions of a covered entity, or that fails to adhere to such instructions, is a covered entity and not a service provider with respect to a specific processing of covered data. A service provider that continues to adhere to the instructions of a covered entity with respect to a specific processing of covered data remains a service provider. If a service provider begins, alone or jointly with others, determining the purposes and means of the processing of covered data, it is a covered entity and not a service provider with respect to the processing of such data.

(3)A covered entity that transfers covered data to a service provider or a service provider that transfers covered data to a covered entity or another service provider, in compliance with the requirements of this chapter, is not liable for a violation of this chapter by the service provider or covered entity to whom such covered data was transferred, if at the time of transferring such covered data, the covered entity or service provider did not have actual knowledge that the service provider or covered entity would violate this chapter.

(4)A covered entity or service provider that receives covered data in compliance with the requirements of this chapter is not in violation of this chapter as a result of a violation by a covered entity or service provider from which such data was received.

(e)A third party:

(1)shall not process third party data for a processing purpose other than the processing purpose for which

(i)the individual gave consent or to effect a purpose enumerated in paragraph (2), (3), or (5) of subsection (a) of section 2 in the case of sensitive covered data; or

(ii)the covered entity made a disclosure pursuant to their privacy policy and in the case of data that is not sensitive covered data; and

(2)may reasonably rely on representations made by the covered entity that transferred the third-party data if the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible.

(f)Solely for the purposes of this section, the requirements for service providers to contract with, assist, and follow the instructions of covered entities shall be read to include requirements to contract with, assist, and follow the instructions of a government entity if the service provider is providing a service to a government entity.

Section 12. Enforcement

(a) A violation of this chapter constitutes an injury to that individual and shall be deemed an unfair or deceptive act or practice in the conduct of trade or commerce under chapter 93A, provided that if the court finds for any petitioner, subject to section 9, paragraph (3) of such chapter, recovery under such chapter shall be in the amount of actual damages or $5,000, whichever is higher.

(b) Private right of action. Any individual alleging a violation of this chapter by a covered entity, service provider, or third party that is a large data holder may bring a civil action in the superior court or any court of competent jurisdiction.

(c) An individual protected by this chapter may 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 under this chapter.

(d) The civil action shall be directed to the covered entity, service provider, and third-parties alleged to have committed the violation.

(e) In a civil action in which the plaintiff prevails, the court may award:

(1)liquidated damages of not less than 0.15% of the annual global revenue of the covered entity or $15,000 per violation, whichever is greater;

(2)punitive damages; and

(3)any other relief, including but not limited to an injunction, that the court deems to be appropriate.

(f) In addition to any relief awarded pursuant to the previous paragraph, the court shall award reasonable attorney's fees and costs to any prevailing plaintiff.

(g) The Attorney General may bring an action pursuant to section 4 of chapter 93A against a covered entity, service provider, or third party to remedy violations of this chapter and for other relief, including but not limited to an injunction, that may be appropriate, subject to the following:

(1) If the court finds that the defendant has employed any method, act, or practice which they knew or should have known to be in violation of this chapter, the court may require the defendant to pay to the commonwealth a civil penalty of:

(i) not less than 0.15% of the annual global revenue or $15,000, whichever is greater, per violation; and

(ii) not more than 4% of the annual global revenue of the covered entity, service provider, or third-party or $20,000,000, whichever is greater, per action if such action includes multiple violations to multiple individuals;

(2) If the court finds that a defendant has engaged in flagrant, willful and repeat violations of this chapter, the court may issue an order to suspend or prohibit a covered entity, service provider, or third party from operating in the commonwealth or collecting, processing, and transferring covered data and any other relief, including but not limited to an injunction, that the court deems to be appropriate.

(3) In addition to any penalty or relief awarded under this subsection, a defendant violating this chapter shall also be liable to the commonwealth for the reasonable costs of investigation and litigation of such violation, including reasonable attorneys' fees and reasonable expert fees.

(h) When calculating awards and civil penalties in all the actions in this section, the court shall consider:

(1) the number of affected individuals;

(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.

(i) It is a violation of this chapter for a covered entity or anyone else acting on behalf of a covered entity to retaliate against an individual who makes a good-faith complaint that there has been a failure to comply with any part of this chapter.

(1) An injured individual by a violation of the previous paragraph may bring a civil action for monetary damages and injunctive relief in any court of competent jurisdiction.

(j) Any provision of a contract or agreement of any kind, including a covered entity's terms of service or a privacy policy, including the short-form privacy notice required under section 9 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.

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

Section 13. Information Non-applicability

(a) This chapter shall not apply to only the following specific types of information:

(1) personal information captured from a patient by a health care provider or health care facility or biometric information collected, processed, used, or stored exclusively for medical education or research, public health or epidemiological purposes, health care treatment, insurance, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996, or to X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used exclusively to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening;

(2) nonpublic personal information that is processed by a financial institution subject to, and in compliance with, the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq., as amended from time to time;

(3) personal information regulated by the federal Family Educational Rights and Privacy Act, 20 U.S.C. 1232g et seq., as amended from time to time;

(4) individuals sharing their personal contact information such as email addresses with other individuals in the workplace, or other social, political, or similar settings where the purpose of the information is to facilitate communication among such individuals, provided that this chapter shall cover any processing of such contact information beyond interpersonal communication; or

(5) covered entities' publication of 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.

(b) For the purpose of this section, the burden of proving that information is exempt from the provisions of this chapter shall be upon the party claiming the exemption.

Section 14. Implementation

(a) The Attorney General shall adopt rules and regulations for the implementation, administration, and enforcement of this chapter and may from time to time amend or repeal said regulations. The rules and regulations shall include but are not limited to:

(1) establishing or adopting baseline technical requirements that determine if a given dataset has been or can be considered sufficiently de-identified;

(2) establishing reasonable policies, practices, and procedures that satisfy the requirements set forward in Section 6;

(3) establishing a nonexclusive list of practices that constitute deceptive designs or dark patterns or otherwise violate the requirements set forward in Section 5; and

(4) further defining when a covered entity is a data broker and additional compliance requirements for data brokers under this chapter.

(b) The Attorney General may:

(1)gather facts and information applicable to the Attorney General's obligation to enforce this chapter and ensure its compliance, consistent with the provisions of section 4 of chapter 93A;

(2) conduct investigations for possible violations of this chapter; and

(3) refer cases for civil enforcement or criminal prosecution to the appropriate federal, state, or local authorities.

(c) The Attorney General shall, within one year after the effective date of chapter, create an official internet website that outlines the provisions of this chapter and provides individuals with a form or other mechanism to report violations of this chapter to the Office of the Attorney General. The Attorney General shall update the website at least annually. The website shall include statistics on the Attorney General's enforcement actions undertaken under this chapter, broken down by fiscal year, including but not limited to:

(1) number of complaints received;

(2) number of open investigations;

(3) number of closed investigations; and

(4) a summary of case dispositions in which a violation of this chapter occurred.

Section 15. Authorized Agents

(a) An individual may designate another person to serve as the individual's authorized agent to exercise the individual's rights under section 4, to withdraw consent under section 10, or opt out of the processing of such individual's covered data for one or more of the purposes specified in section 10.

(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 10.

(c) A covered entity or service provider shall comply with a request received from an authorized agent if the covered entity or service provider is able to verify the identity of the individual and the authorized agent's authority to act on such individual's behalf by the same means and subject to the same restrictions as a covered entity under section 4(g).

(d) In the case of covered data concerning an individual known to be a child as defined by the Children's Online Privacy Protection Act, 15 U.S.C. 6501, the parent or legal guardian of such child may exercise the rights provided under this chapter on the child's behalf.

(e) In the case of covered data concerning an individual subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the individual may exercise the rights provided under this chapter on the individual's behalf.

Section 16. Advertising to Minors

(a) A covered entity or service provider may not engage in targeted advertising to any individual if the covered entity has knowledge that the individual is a minor.

Section 17. Data Brokers

(a)Each data broker shall place a clear, conspicuous, not misleading, and readily accessible notice on the website or mobile application of the data broker (if the data broker maintains such a website or mobile application) that:

(1)notifies individuals that the entity is a data broker;

(2)includes a link to the data broker registry website; and

(3)is reasonably accessible to and usable by individuals with disabilities.

(b)Data broker registration. Not later than January 31 of each calendar year that follows a calendar year during which a covered entity acted as a data broker, data brokers shall register with the OCABR in accordance with this subsection.

(1)In registering with the OCABR, a data broker shall do the following:

(i)Pay to the OCABR a registration fee of $100;

(ii)Provide the OCABR with the following information:

(A)The legal name and primary physical, email, and internet addresses of the data broker;

(B)A description of the categories of covered data the data broker processes and transfers;

(C) The contact information of the data broker, including a contact person, a telephone number, an e-mail address, a website, and a physical mailing address; and

(D) A link to a website through which an individual may easily exercise the rights provided under this subsection.

(c)The OCABR shall establish and maintain on a website a searchable, publicly available, central registry of third-party collecting entities that are registered with the OCABR under this subsection that includes a listing of all registered data brokers and a search feature that allows members of the public to identify individual data brokers and access to the registration information provided under subsection (b).

(d)Penalties. A data broker that fails to register or provide the notice as required under this section shall be subject to enforcement proceedings under section 12.

Section 18. Severability and Relationship to Other Laws

(a) Should any provision of this chapter or part hereof be held under any circumstances in any court of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect the validity or enforceability of any other provision of this or other parts of this chapter.

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

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

Chapter 93N. Privacy Protections for Location Information Derived from Electronic Devices

Section 1. Definitions

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

(1) "Application", a software program that runs on the operating system of a device.

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

(3) "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.

(4) "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 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. Effective Date

This Act shall take effect 1 year after enactment.