SENATE DOCKET, NO. 745 FILED ON: 1/18/2023

SENATE . . . . . No. 25

The Commonwealth of Massachusetts

PRESENTED BY:

Cynthia Stone Creem

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act establishing the Massachusetts Data Privacy Protection Act.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	
Cynthia Stone Creem	*Norfolk and Middlesex*	
Jason M. Lewis	*Fifth Middlesex*	*2/9/2023*

SENATE DOCKET, NO. 745 FILED ON: 1/18/2023

SENATE . . . . . No. 25

By Ms. Creem, a petition (accompanied by bill, Senate, No. 25) of Cynthia Stone Creem and Jason M. Lewis for legislation to establish the Massachusetts Data Privacy Protection Act. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

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

An Act establishing the Massachusetts Data Privacy Protection 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 2020 Official Edition, are hereby amended by inserting after chapter 93K the following chapter:

Chapter 93L. Massachusetts Data Privacy Protection 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)affirmative express consent”, an affirmative act by an individual that clearly communicates the individual’s freely given, specific, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a covered entity that meets the requirements of this chapter.

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

(3)“biometric information”, any covered 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:—

(i)fingerprints;

(ii)voice prints;

(iii)iris or retina scans;

(iv)facial or hand mapping, geometry, or templates; or

(v)gait or personally identifying physical movements.

The term “biometric information” does not include a digital or physical photograph; an audio or video recording; or data generated from a digital or physical photograph, or an audio or video recording, that cannot be used to identify an individual.

(4)“collect” and “collection”, buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means.

(5)“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.

(6)“covered algorithm”, a computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity and that makes a decision or facilitates human decision-making with respect to covered data, including determining the provision of products or services or to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to an individual.

(7) “covered data”, information, including derived data 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. The term “covered data” does not include:—

(i)de-identified data;

(ii)employee data covered under section 204 of chapter 149 of the general laws; or

(iii)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 75,000 individuals during the period beyond 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.

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

(11) “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.

(12)“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.

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

(14)“first party advertising or marketing”, advertising or marketing conducted by a covered entity that collected covered data from the individual through either direct communications with the individual such as direct mail, email, or text message communications, or advertising or marketing conducted entirely within the first-party context, such as in a physical location operated by or on behalf of such covered entity, or on a web site or app operated by or on behalf of such covered entity.

(15)“genetic information”, any covered data, regardless of its format, that concerns an individual’s genetic characteristics, including:—

(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 (A).

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

(17)“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 covered 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 covered 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.

(18)“large data holder”, a covered entity or service provider that in the most recent calendar year:—

(i)had annual gross revenues of $250,000,000 or more; and

(ii)collected, processed, or transferred the covered data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to 1 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; and the sensitive covered data of more than 200,000 individuals or devices that identify or are linked or reasonably linkable to 1 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.

(19)“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;

(20)“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.

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

(22 “process”, to conduct or direct any operation or set of operations performed on covered data, including analyzing, organizing, structuring, retaining, storing, using, or otherwise handling covered data.

(23 “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.

(24)“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 restricted the information to a specific audience.

The term "publicly available information" does not include:—

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

(ii)any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive

(iii) covered data with respect to an individual;

(iv)biometric information;

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

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

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

(25)“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.

(26)“sensitive covered data”, the following types of covered data:—

(i)a government-issued identifier, such as a Social Security number, passport number, or driver’s license number, that is not required by law to be displayed in public.

(ii)any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual.

(iii)a financial account number, debit card number, credit card number, or information that describes or reveals the income level or bank account balances of an individual, except that the last four digits of a debit or credit card number shall not be deemed sensitive covered data.

(iv)biometric information.

(v)genetic information.

(vi)location information.

(vii)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.

(viii) account or device log-in credentials, or security or access codes for an account or device.

(ix) information identifying the sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding the collection, processing, or transfer of such information or when it is processed in a way that creates a substantial privacy risk for the individual.

(x)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.

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

(xii)information revealing the video content requested or selected by an individual collected by a covered entity that is not a provider of a service described in section 102(4). This clause does not include covered data used solely for transfers for independent video measurement.

(xiii)information about an individual when the covered entity or service provider has knowledge that the individual is a covered minor.

(xiv)an individual's race, color, ethnicity, sex, gender identity, sexual orientation, national origin, immigration status, disability, religion, or union membership.

(xv) information identifying 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 (1) through (16).

(27) "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.

(28)“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.

(29) “small business”, a covered entity or a service provider 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):—

(i)the covered entity or service provider’s average annual gross revenues during the period did not exceed $41,000,000;

(ii)the covered entity or service provider, on average, did not annually collect or process the covered data of more than 200,000 individuals during the period beyond 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

(iii)the covered entity or service provider did not derive more than 50 percent of its revenue 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.

(30) “substantial privacy risk”, the collection, processing, or transfer of covered data in a manner that may result in any reasonably foreseeable substantial physical injury, economic injury, highly offensive intrusion into the privacy expectations of a reasonable individual under the circumstances, or discrimination on the basis of race, color, religion, national origin, sex, sexual orientation, gender identity or disability.

(31) “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; and 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 in which the advertisement appears and does not vary based on who is viewing the advertisement; or

(iii)processing covered data solely for measuring or reporting advertising or content, performance, reach, or frequency, including independent measurement.

(32) “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.

(33)"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.

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

(35)"transfer", to disclose, 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 affirmative express 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 may not collect, process, or tran sfer 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;

(13)to support or promote participation by individuals in civic engagement activities and democratic governance, including voting, petitioning, engaging with government proceedings, providing indigent legal aid services, and unionizing; or

(14)transfer assets to a third party in the context of a merger, acquisition, bankruptcy, or similar transaction when the third party assumes control, in whole or in part, of the 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 may, with respect to covered data previously collected in accordance with the previous subsection, process such data:—

(1) as necessary to provide first-party advertising or marketing of products or services provided by the covered entity for individuals who are not covered minors;

(2)to provide targeted advertising; provided, however, that such collection, processing, and transferring complies with the requirements of this chapter;

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

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

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

(6)perform inventory management or reasonable network management;

(7)protect against spam; or

(8)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 design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision-making, or choice.

(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), (14) 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 affirmative express 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 re-used 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; and

(vi)in the case of transfer assets in case of a merger, if the transfer is made in accordance with paragraph (14) of subsection (a) of section (2); or

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

Section 4. Consent practices

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

(1)The request for affirmative consent should 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 only if the product or service is not offered in a medium that 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; and

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

(b)A covered entity shall not infer that an individual has provided affirmative express 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 affirmative express consent of an individual through:—

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

(2)the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision-making, or choice to provide such consent or any covered data.

Section 5. Privacy by design

(a)A covered entity and a 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 covered minors;

(3)mitigate privacy risks, including substantial 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; and

(4)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, including substantial 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 and a 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 6. 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 subsection, no covered entity may offer different types of pricing that are unjust, unreasonable, coercive, or usurious in nature.

Section 7. Privacy policy

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

(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, the following:—

(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;

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

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

(v)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;

(vi)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;

(vii)A prominent description of how an individual can exercise the rights described in this chapter;

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

(ix)The effective date of the privacy policy.

(d)If a covered entity makes a material change to its privacy policy or practices, the covered entity 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 (15) of section 2, 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)The covered entity 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 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.

Section 8. Individual data 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, 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 24 months preceding the request;

(ii)the categories of any third party, 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 for consideration 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

(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 design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to exercise such right.

(c)Subject to subsections (d) and (e), each request under subsection (a) shall be completed within 30 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual.

(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 30-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:—

(A)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

(B)any time beyond the initial two times described in subparagraph (A), 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 individual 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 (or an individual authorized to make such a request on the individual's behalf), 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 de-identified data;

(4)require the covered entity to maintain covered data in an identifiable form or 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 interfere 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)involves private elementary and secondary schools as defined by state law and private institutions of higher education as defined by title I of the Higher Education Act of 1965 and targets covered data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution.

(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 covered 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.

Section 9. Advanced data rights.

(a)Covered entities shall provide an individual with a clear and conspicuous, easy-to-execute means to withdraw affirmative express consent. Those means shall be as easy to execute by a reasonable individual as the means to provide consent.

(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 objects to the transfer; and

(2)shall allow an individual to object to such a transfer through an opt out mechanism, as described in section 12.

(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 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.

(d)A covered entity or service provider that receives an opt-out notification pursuant to this section shall abide by such opt-out designations by an individual and notify any other person that directed the covered entity or service provider to serve, deliver, or otherwise handle the advertisement of the opt-out decision.

(e)A covered entity 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 design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to exercise any such right.

(f)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.

Section 10. Minors

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

Section 11. 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 liable for:—

(1)a civil penalty of $100 for each day the data broker fails to register or provide notice as required under this section, not to exceed a total of $10,000 for any year; and

(2)an amount equal to the registration fees for each year that the data broker failed to register as required under this subsection.

(e)Nothing in this subsection shall be construed as altering, limiting, or affecting any enforcement authorities or remedies under this chapter.

Section 11. 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 or disability.

(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 (14) this chapter.

(1)Not later than 3 years after the date of enactment of this chapter, and annually thereafter, the Attorney General shall submit to the legislature a report that includes a summary of the enforcement actions taken under this subsection.

(d)Covered algorithm impact and evaluation. Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this chapter, and annually thereafter, a large data holders that uses a covered algorithm in a manner that poses a consequential risk of harm to an individual or group of individuals, and uses such covered algorithm solely or in part, to collect, process, or transfer covered data or publicly available data shall conduct an impact assessment of such algorithm in accordance with paragraph (1).

(1)The impact assessment required under subsection (d) shall provide the following:—

(i)A detailed description of the design process and methodologies of the covered algorithm;

(ii)A statement of the purpose and proposed uses of the covered algorithm;

(iii)A detailed description of the data used by the covered algorithm, including the specific categories of data that will be processed as input and any data used to train the model that the covered algorithm relies on, if applicable;

(iv)A description of the outputs produced by the covered algorithm as well as the outcomes of their use;

(v)An assessment of the necessity and proportionality of the covered algorithm in relation to its stated purpose; and

(vi)A detailed description of steps the large data holder has taken or will take to mitigate potential harms from the covered algorithm to an individual or group of individuals, including related to:—

(A)covered minors;

(B)making or facilitating advertising for, or determining access to, or restrictions on the use of housing, education, employment, healthcare, insurance, or credit opportunities;

(C)determining access to, or restrictions on the use of, any place of public accommodation, particularly as such harms relate to the protected characteristics of individuals, including race, color, religion, national origin, sex, sexual orientation, gender identity or disability;

(D)disparate impact on the basis of individuals' race, color, religion, national origin, sex, sexual orientation, gender identity or disability status; or

(E)disparate impact on the basis of individuals' political party registration status.

(e)Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this chapter, a covered entity or service provider that knowingly develops a covered algorithm that is designed, solely or in part, to collect, process, or transfer covered data in furtherance of a consequential decision shall, prior to deploying the covered algorithm evaluate the design, structure, and inputs of the covered algorithm, including any training data used to develop the covered algorithm, to reduce the risk of the potential harms identified under the previous paragraph.

(f)In complying with paragraphs (1) and (2), a covered entity and a service provider may focus the impact assessment or evaluation on any covered algorithm, or portions of a covered algorithm, that will be put to use and may reasonably contribute to the risk of the potential harms identified under paragraph (2).

(g)A covered entity and a service provider shall:—

(1)submit the impact assessment or evaluation conducted under paragraph (1) or (2) to the Attorney General not later than 30 days after completing an impact assessment or evaluation;

(2)make such impact assessment and evaluation available to the legislature, upon request; and

(3)make a summary of such impact assessment and evaluation publicly available in a their website or any other similar place that is easily accessible to individuals.

(h)Covered entities and service providers may redact and segregate any trade secrets, as defined in 18 U.S.C. section 1839, or other confidential or proprietary information from public disclosure under this subsection.

(i)The Attorney General may not use any information obtained solely and exclusively through a covered entity or a service provider's disclosure of information to the Attorney General in compliance with this section for any other purpose than enforcing this chapter; provided, however, that it may be used for enforcing consent orders.

(1)The previous subparagraph does not preclude the Attorney General from providing information about a covered entity to the legislature in response to a subpoena.

Section 12. Miscellaneous

(a)Not later than 18 months after the date of enactment of this chapter, the OCABR shall establish or recognize one or more acceptable privacy protective, centralized mechanisms for individuals to exercise the opt-out rights recognized in section 9.

(b)Any such centralized opt-out mechanism shall:—

(1)require covered entities or service providers acting on behalf of covered entities to inform individuals about the centralized opt-out choice;

(2)not be required to be the default setting, but may be the default setting provided that in all cases the mechanism clearly represents the individual's affirmative, freely given, and unambiguous choice to opt out;

(3)be consumer-friendly, clearly described, and easy-to-use by a reasonable individual;

(4) be provided in any covered language in which the covered entity provides products or services subject to the opt-out; and

(5)be provided in a manner that is reasonably accessible to and usable by individuals with disabilities.

(c)A covered entity or service provider that is not a small business shall designate:—

(1)1 or more qualified employees as privacy officers; and

(2)1 or more qualified employees as data security officers.

(d)An employee who is designated as a privacy officer or a data security officer pursuant to subsection (c) shall, at a minimum:—

(1)implement a data privacy program and data security program to safeguard the privacy and security of covered data in compliance with the requirements of this chapter; and

(2)facilitate the covered entity or service provider's ongoing compliance with this chapter.

(e)Each covered entity that is a large data holder shall conduct a privacy impact assessment that weighs the benefits of the large data holder's covered data collecting, processing, and transfer practices against the potential adverse consequences of such practices, including substantial privacy risks, to individual privacy.

(1)The assessment shall be conducted not later than 1 year after the date of enactment of this chapter or 1 year after the date on which a covered entity first meets the definition of large data holder, whichever is earlier, and biennially thereafter.

(f)A privacy impact assessment required under subsection (e) shall be:—

(1)reasonable and appropriate in scope given:—

(i)the nature of the covered data collected, processed, and transferred by the large data holder;

(ii)the volume of the covered data collected, processed, and transferred by the large data holder; and

(iii)the potential material risks posed to the privacy of individuals by the collecting, processing, and transfer of covered data by the large data holder;

(2)documented in written form and maintained by the large data holder unless rendered out of date by a subsequent assessment conducted under subsection (e); and

(3)approved by the privacy protection officer designated pursuant to subsection (c).

(g)In assessing the privacy risks, including substantial privacy risks, the large data holder must include reviews of the means by which technologies are used to secure covered data.

Section 13. 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, providing information necessary to enable the covered entity to conduct and document a privacy impact assessment required by this chapter;

(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 (15) 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 affirmative express 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 data;

(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 14. Enforcement. Private Right of Action and Attorney General enforcement.

(a)A violation of this chapter or a regulation promulgated under this chapter constitutes an injury to that individual.

(b)Private right of action. Any individual alleging a violation of this chapter by a covered entity that is not a small business 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 commission or to accept mandatory arbitration of a claim under this chapter.

(d)The civil action shall be directed to the covered entity, data processor, and the 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, third party or data broker to remedy violations of this chapter and for other relief that may be appropriate.

(1)If the court finds that the defendant has employed any method, chapter, or practice which they knew or should have known to be in violation of this chapter, the court may require such person 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, data processor, or third-party or $20,000,000, whichever is greater, per action if such action includes multiple violations to multiple individuals;

(2)All money awards shall be paid to the commonwealth. The commonwealth shall identify the individuals affected by the violation and earmark such money awards, penalties, or

assessments collected for purposes of paying for the damages they suffered as a consequence of the violation.

(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.

Section 15. Enforcement - Miscellaneous

(a)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 3 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.

(b)No covered entity that is a provider of an interactive computer service, as defined in 47 U.S.C. section 230, shall be treated as the publisher or speaker of any personal information provided by another information content provider, as defined in 47 U.S.C. section 230 and allowing posting of information by a user without other action by the interactive computer service shall not be deemed processing of the personal information by the interactive computer service.

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

Section 16. Transparency

(a)Covered entities that receive any form of a legal request for disclosure of personal information pursuant to this chapter shall:—

(1)provide the Attorney General and the general public a bi-monthly report containing the following aggregate information related to legal requests received by the covered entity, their affiliated data processors, and any third parties they contracted with:—

(i)The total number of legal requests, disaggregated by type of requests such as warrants, court orders, and subpoenas;

(ii)The number of legal requests that resulted in the covered entity disclosing personal information;

(iii)The number of legal requests that did not result in the covered entity disclosing personal information, including the reasons why the information was not disclosed;

(iv)The type of personal information sought in the legal requests received by the covered entity;

(v)The total number of legal requests seeking the disclosure of location or biometric information;

(vi)The number of legal requests that resulted in the covered entity disclosing location or biometric information;

(vii)The number of legal requests that did not result in the covered entity disclosing location or biometric information, including the reasons for such no disclosure; and

(viii)The nature of the proceedings from which the requests were ordered and whether it was a government entity or a private person seeking the legal request;

(b)take all reasonable measures and engage in all legal actions available to ensure that the legal request is valid under applicable laws and statutes; and

(c)require their affiliate data processors and third parties they contracted with to have similar practices and standards.

Section 17. Non-applicability

(a)This chapter shall not apply to:—

(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 chapter 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)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

(3)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.

Section 18. Relationship with other laws

(a)Nothing in this chapter shall diminish any individual's rights or obligations under the Massachusetts Fair Information Practices chapter and its regulations.

Section 19. Implementation

(a)The Attorney General shall:—

(1)adopt, amend, or repeal regulations for the implementation, administration, and enforcement of this chapter;

(2)gather facts and information applicable to the Attorney General's obligation to enforce this chapter and ensure its compliance;

(3)conduct investigations for possible violations of this chapter;

(4)refer cases for criminal prosecution to the appropriate federal, state, or local authorities; and

(5)maintain an official internet website outlining the provisions of this Act.

Section 20. Severability

(a)Should any provision of this chapter or part hereof be held under any circumstances in any 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.

SECTION 2. Chapter 149 of the General Laws, as appearing in the 2018 Official Edition, is hereby amended by inserting after section 203 the following section:—

Section 204. Workplace Surveillance

(a)For the purposes of this section, the following words shall have the following meanings unless the context clearly requires otherwise:—

(1)"Information" also referred to as "employee information," or "employee data", information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular employee, regardless of how the information is collected, inferred, or obtained.

(2)"Electronic monitoring", the collection of information concerning employee activities, communications, actions, biometrics, or behaviors by electronic means.

(3)"Employment-related decision", any decision made by the employer that affects wages, benefits, hours, work schedule, performance evaluation, hiring, discipline, promotion, termination, job content, productivity requirements, workplace health and safety, or any other terms and conditions of employment.

(4)"Vendor", a business engaged in a contract with an employer to provide services, software, or technology that collects, stores, analyzes, or interprets employee information.

(5)“Facial recognition technology” shall have the meaning established in section 220 of chapter 6 of the General Laws, as amended by Chapter 253 of the Acts of 2020.

(b)An employer, or vendor acting on behalf of an employer, shall not electronically monitor an employee unless:—

(1)the electronic monitoring only purpose is to:—

(i)enable tasks that are necessary to accomplish essential job functions;

(ii)monitor production processes or quality;

(iii)comply with employment, labor, or other relevant laws;

(iv)protect the safety and security of employees; or

(v)carry on other purposes as determined by the department of labor standards; and

(2)the specific form of electronic monitoring is:—

(i)necessary to accomplish the allowable purpose;

(ii)the least invasive means that could reasonably be used to accomplish the allowable purpose;

(iii)limited to the smallest number of employees; and

(iv)collecting the least amount of information necessary to accomplish the purpose mentioned in (1).

(c)Notwithstanding subsection (b), the following practices shall be prohibited:—

(1)use of electronic monitoring that either directly or indirectly harms an employee's physical health, mental health, personal safety or wellbeing;

(2)monitoring of employees who are off-duty and not performing work-related tasks;

(3)audio-visual monitoring of bathrooms or other similarly private areas including locker rooms and changing areas;

(4)audio-visual monitoring of break rooms, lounges, and other social spaces, except to investigate specific illegal activity;

(5)use of facial recognition technology other than for the purpose of verifying the identity of an employee for security purposes; and

(6)any other forms of electronic monitoring such as may be prohibited by the department of labor standards.

(d)Employers shall not require employees to install applications on personal or mobile devices that collect employee information or require employees to wear data-collecting devices, including those that are incorporated into items of clothing or personal accessories, unless the electronic monitoring is necessary to accomplish essential job functions and is narrowly limited to only the activities and times necessary to accomplish essential job functions.

(e)Information resulting from electronic monitoring shall be accessed only by authorized agents and used only for the purpose and duration for which notice was given in accordance with subsection (f).

(f)Employers shall provide employees with notice that electronic monitoring will occur prior to conducting each specific form of electronic monitoring. The notice must, at a minimum, include:—

(1)a description of:—

(i)the purpose that the specific form of electronic monitoring is intended to accomplish, as specified in subsection (b);

(ii)the specific activities, locations, communications, and job roles that will be electronically monitored;

(iii)the technologies used to conduct the specific form of electronic monitoring;

(iv)the vendors or other third parties that information collected through electronic monitoring will be disclosed or transferred to, including the name of the vendor and the purpose for the data transfer;

(v)the organizational positions that are authorized to access the information collected through the specific form of electronic monitoring, and under what conditions; and

(vi)the dates, times, and frequency that electronic monitoring will occur;

(2)the names of any vendors conducting electronic monitoring on the employer’s behalf; and

(3)an explanation of:—

(i)the reasons why the specific form of electronic monitoring is necessary to accomplish the purpose; and

(ii)how the specific monitoring practice is the least invasive means available to accomplish the allowable monitoring purpose.

(g)The notice mentioned in (f) shall be clear and conspicuous and provide the employee with actual notice of electronic monitoring activities.

(1)A notice that provides electronic monitoring "may" take place or that the employer "reserves the right" to monitor shall not suffice.

(h)An employer who engages in random or periodic electronic monitoring of employees will inform the affected employees of the specific events which are being monitored at the time the monitoring takes place with a notice that shall be clear and conspicuous.

(1)Notwithstanding the previous paragraph, notice of random or periodic electronic monitoring may be given after electronic monitoring has occurred only if necessary to preserve the integrity of an investigation of wrongdoing or protect the immediate safety of employees, customers, or the public.

(i)Employers shall provide a copy of the above notice disclosure to the department of labor standards.

(j)An employer shall only use employee information collected through electronic monitoring to accomplish its purpose, unless the information documents illegal activity.

(k)When making a hiring or employment-related decision using information collected through electronic monitoring, an employer shall:—

(1)not make the decision based solely on such information;

(2)give the affected employee access to the data and provide an opportunity to correct or explain it;

(3)corroborate such information by other means, such as independent documentation by supervisors or managers, or by consultation with other employees; and

(4)document and communicate to affected employees the basis for the corroboration prior to the decision going into effect.

(l)Subsection (k) shall not apply to those cases when electronic monitoring data provides evidence of illegal activity.

SECTION 3. Effective date.

(a)The provisions of this Act shall take effect 12 months after this Act is enacted.

(b)The enforcement of chapter 93L shall be delayed until 6 months after the effective date.