SENATE DOCKET, NO. 1726 FILED ON: 2/18/2021

SENATE . . . . . No. 46

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 Information Privacy Act.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	
Cynthia Stone Creem	*First Middlesex and Norfolk*	
Eric P. Lesser	*First Hampden and Hampshire*	*3/15/2021*

SENATE DOCKET, NO. 1726 FILED ON: 2/18/2021

SENATE . . . . . No. 46

By Ms. Creem, a petition (accompanied by bill, Senate, No. 46) of Cynthia Stone Creem and Eric P. Lesser for legislation to establish the Massachusetts Information Privacy Act. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Second General Court
(2021-2022)

An Act establishing the Massachusetts Information 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 2018 Official Edition, are hereby amended by inserting after chapter 93K the following chapter:

CHAPTER 93L. Massachusetts Information 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:—

“Advertisement” means the process by which a person, the “advertiser,” proposes a commercial transaction or disseminates a public or private communication or message to solicit business or a commercial opportunity.

“Algorithm” means a specific procedure, set of rules, or order of operations designed to solve a problem or make a calculation, classification, or recommendation.

"Artificial intelligence" means computerized methods and tools, including but not limited to machine learning and natural language processing, that act in a way that resembles human cognitive abilities when it comes to solving problems or performing certain tasks.

"Automated decision system" means any computer program, method, statistical model, or process that aims to aid or replace human decision-making using algorithms or artificial intelligence. These systems can include analyzing complex datasets about human populations to generate scores, predictions, classifications, or recommendations used to make decisions.

"Biometric information" means information that pertains to measurable biological or behavioral characteristics of an individual that can be used singularly or in combination with each other or with other information for automated recognition or identification of a known or unknown individual. Examples include but are not limited to fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, gait, handwriting, keystroke dynamics, and mouse movements.

Biometric information does not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.

Biometric information does not include donated organs, tissues, or parts, or blood, or serum stored on behalf of recipients or potential recipients of living, or cadaveric transplants obtained or stored by a federally designated organ procurement agency.

Biometric information does not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.

Biometric information does not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Browser personal information" means Internet Protocol addresses, system configuration information, Uniform Resource Locators of referring pages, local and language preferences, keystrokes, and other similar digital sources associated with an individual.

"Collect" means to collect, buy, rent, gather, obtain, receive, trade for, or access any personal information pertaining to an individual by any means, online or offline, including, but not limited to receiving information from the individual or a third-party, actively or passively, or obtaining information by observing the individual's behavior.

"Conduct business in the Commonwealth of Massachusetts" or "conducting business in Massachusetts" means to produce, solicit, or offer for use or sale any information, product, or service in a manner that intentionally targets or may reasonably be expected to contact individuals.

"Consent" means freely given, specific, informed, unambiguous, opt-in consent by individuals.

"Commission" means the Massachusetts information privacy commission established by section 79 of chapter 10.

"Covered entity" means an entity that conducts business in the Commonwealth of Massachusetts, processes personal information by itself or by contracting with a data processor,

and (i) has earned or received 10 million or more dollars of annual revenue through 300 or more transactions, or (ii) processes or maintains the personal information of 10,000 or more unique individuals during the course of a calendar year.

"Covered interaction" means an interaction between an individual or its household and a covered entity when such covered entity makes available information, products, or services to the individual and collects or otherwise processes personal information pertaining to that individual. Covered interactions include but are not limited to posting information, offering a product or service, the placement of targeted advertisements, setting up an account, or offering membership or other ongoing relationship with a covered entity.

"Data processor" means a person or entity that processes personal information on behalf of a covered entity.

"De-identified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be directly linked to a particular individual or household.

"Device" means a tool that is capable of sending, routing, or receiving communications to or from another device and intended for use by a single individual or single household or, if used outside of a home, for use by the general public.

"Disclose" means any action, set of actions, or omission in which a covered entity, data processor, or a third-party makes personal information available to another person, intentionally or unintentionally, including but not limited to sharing, publishing, releasing, transferring, disseminating, making available, selling, leasing, providing access to, failing to restrict access to, or otherwise communicating orally, in writing, electronically, or by any other means.

"Entity" means the following entities as defined in section 1.40 of chapter 156D:

i. "Corporation", "domestic corporation" or "domestic business corporation";

ii. "Other entity"; and

iii. "Foreign business corporation" or "foreign other entity".

This term does not include Massachusetts governmental entities.

"Harm" shall mean potential or realized adverse consequences for an individual or society, including but not limited to:—

i. Direct or indirect financial harm;

ii. Physical harm or threats to individuals or property, including but not limited to bias-related crimes and threats, harassment, and sexual harassment;

iii. Discrimination in products, services, or economic opportunities such as housing, employment, credit, insurance, education, or health care on the basis of an individual or class of individuals belonging to, or being perceived as belonging to, one of the protected classes under section 4 of chapter 151B, except as specifically authorized by law;

iv. Interference with or surveillance of First Amendment-protected activities by state actors, except as specifically authorized by law;

v. Interference with the right to vote or with free and fair elections;

vi. Violation of individuals' rights to due process or equal protection under the law;

vii. Loss of individual control over personal information via non-consensual sharing of sensitive personal information, data breach, or other actions that violate this chapter;

viii. The non-consensual capture of information or communications within an individual's home or where an individual is entitled to have a reasonable expectation of privacy or access control;

ix. Other effects on an individual that may not be reasonably foreseeable to, contemplated by or expected by the individual to whom the personal information relates, which are nevertheless reasonably foreseeable to, contemplated by, or expected by the covered entity, that alter or limit that individual's choices or predetermine results.

"Individual" means a natural person who is a resident of the Commonwealth of Massachusetts. The location of a natural person in the Commonwealth of Massachusetts shall create a presumption that the natural person is a Commonwealth of Massachusetts resident.

"Legal request" means any request for personal information issued by a court of competent jurisdiction pursuant to state or federal laws such as subpoenas, court orders, search warrants, pen register and trap and trace orders, or wiretap orders.

"Location information" means information pertaining to where an individual has physically been or directly or indirectly reveals an individual's physical location or the location of a device associated with that individual. Location information includes but is not limited to:-

i. IP addresses;

ii. GPS coordinates;

iii. Cell-site location information;

iv. Time-stamped video or other surveillance information that identifies an individual as being in a certain place;

v. Information derived from transportation cards;

vi. Information related to an individual's visit to certain locations.

"Massachusetts governmental entity" shall mean any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or of any political subdivision thereof, or of any authority established by the general court to serve a public purpose.

"Monetize" or "monetization" means to sell, rent, release, disclose, disseminate, trade, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, an individual's personal information by a covered entity, a third-party, or a data processor in exchange for monetary or other consideration, as well as to leverage or use an individual's personal information to place a targeted advertisement or to otherwise profit, regardless of whether the individual's personal information changes hands.

"Person" means any natural or legal person.

"Personal information" means information about an individual directly or indirectly captured in a covered interaction. Personal information includes any information so captured that directly or indirectly identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to a particular individual, household, or device. Information is reasonably linkable to an individual, household, or device if used on its own or in combination with other reasonably available information to identify an individual, household, or device, regardless of

whether the covered entity holds such additional information. This definition includes but is not limited to the following information:

i. First name, middle names, last names, aliases, and social media and website-used usernames;

ii. Government-issued ID and vehicle license plate numbers;

iii. Telephone numbers, including cellphone numbers, and physical and digital addresses such as IP address and email address;

iv. Date of birth, age, gender, race, ethnicity, national origin, and sexual orientation;

v. Information revealing political opinions, religious, or philosophical beliefs held by identified individuals;

vi. Technical identifiers such as a service ID number that can be tied back to an individual;

vii. Biometric information;

viii. Location information;

ix. Medical and health information including an individual's medical history and search queries related to medical conditions;

x. Financial data, including social security number, details of financial and commercial transactions, and credit scores related to the financial capacity of an individual;

xi. Professional data, including resume, job history, and other similar records related to an individual;

xii. Information pertaining to an individual behavior online, such as a record of the websites they visit or the files they download;

xiii. Browser personal information;

xiv. Information pertaining to an individual's sex life; and

xv. Electronic communications such as messaging, email, and voice conversations;

"Processing" or "process" means any action or set of actions performed on or with personal information, including but not limited to collecting, accessing, using, storing, retaining, sharing, monetizing, analyzing, creating, generating, aggregating, altering, correlating, operating on, decision-making, recording, modifying, organizing, structuring, disclosing, transmitting, selling, licensing, disposing of, destroying, de-identifying, or another handling of personal information. This term includes using personal information in automated decision systems.

"Reasonably understandable" means of length and complexity such that an individual with an eighth-grade reading level, as established by the department of education, can read and comprehend.

"Sensitive personal information" means the following personal information related to an identified individual:—

i. Race, ethnicity, national origin, and sexual orientation;

ii. Date of birth;

iii. Cellphone number;

iv. Information revealing political opinions, religious or philosophical beliefs held by identified individuals;

v. Biometric information;

vi. Location information;

vii. Medical and health information including an individual's medical history and search queries related to medical conditions;

viii. Information pertaining to an individual's sex life;

ix. Social security number; and

x. Credit scores related to the financial capacity of an individual.

"Targeted advertisement" means an advertisement directed to an individual or a group of individuals where the advertisement is selected by an automated decision system based on processed personal information obtained or inferred over time from the individual or the groups of individual's devices activities, communications, or associations across websites, applications, services, or covered entities. It does not include advertisements directed to an individual solely based upon the individual's current visit to a website, application, service, covered entity, or a direct response to the individual's request for information or feedback.

"Third-party" means, with respect to an individual's personal information, any person or governmental entity that is not the covered entity or a data processor.

"Use model" means a discrete purpose for which collected personal information is to be processed, including but not limited to first-party marketing, third-party marketing, first-party research and development, third-party research and development, and product improvement and development.

(b) The commission may adopt regulations, from time to time, to revise the aforementioned definitions, as used in this chapter, to reflect applicable technological advancements.

Section 2. General principles and duties

(a) The provisions of this chapter and the regulations enacted thereof shall be interpreted and administered in accordance with the following general principles:—

1. Covered entities and data processors must process personal information and use automated decision systems discreetly and honestly, and only to the extent necessary for carrying out their purpose; and

2. Covered entities and data processors must be protective of personal information, loyal to the individuals whose personal information is processed, and honest about the risk of processing practices, including the use of automated decision systems.

(b) Duty of Care. Covered entities and data processors shall:—

1. reasonably secure individual personal information from unauthorized access; and

2. promptly comply with chapter 93H of the general laws in case of a breach of security, as defined therein.

(c) Duty of Loyalty. Covered entities and data processors shall not use personal information, or information derived from personal information, in any way that:—

1. benefits themselves to the detriment of an individual;

2. results in reasonably foreseeable and material physical or financial harm to an individual; or

3. would be unexpected and highly offensive to a reasonable individual that provided consent in accordance with this chapter.

(d) Duty of Confidentiality. Covered entities and data processors:—

1. shall not disclose or sell personal information to, or share personal information with, any other person except as consistent with the provisions set forth in this chapter and regulations enacted to implement them;

2. shall not disclose or sell personal information to, or share personal information with, any third-party unless that third-party enters into a contract with the covered entity that imposes on the third-party the same duties of care, loyalty, and confidentiality toward the applicable individual as are imposed on the covered entity under this chapter; and

3. shall take reasonable steps to ensure that the practices of any third-party to whom the covered entity discloses or sells, or with whom the covered entity shares personal information fulfill the duties of care, loyalty, and confidentiality assumed by the third-party under the contract described in the previous paragraph.

i. Covered entities shall regularly audit the data security and data information practices of any such third-party, making such audit publicly available.

Section 3. Rights of access, correction, data portability, and deletion

(a) Access to and Portability of Personal Information

1. Individuals shall have the right to:—

i. access all their personal information that was processed by the covered entity or a data processor;

ii. access all the information pertaining to the collection and processing of their personal information, including but not limited to—

1. where or from whom the covered entity obtained personal information, i.e., from the individual or a third-party, whether online or offline;

2. the types of third parties to which the covered entity has disclosed or will disclose captured personal information;

3. the purposes of the processing;

4. the categories of personal information concerned;

5. the names of third parties to which the covered entity had disclosed the personal information and a log showing when such disclosure happened; and

6. the period of retention of the personal information.

iii. obtain their personal information processed by a covered entity in a structured, readily usable, portable, and machine-readable format;

iv. transmit or cause the covered entity to transmit the personal information to another covered entity, where technically feasible;

v. request a covered entity to stop collecting and processing their personal information.

(b) Correction and Deletion of Personal Information

1. Individuals shall have the right to:—

i. correct inaccurate personal information stored by covered entities; and

ii. delete all their personal information stored by covered entities, provided that a covered entity that has collected personal information from an individual is not required to delete information to the extent it is exempt under this chapter from the requirement of consent.

2. A covered entity that maintains an individual's personal information in a non-public profile or account must correct or delete such personal information, and any information derived therefrom pertaining to the individual upon the individual's request.

(c) Exercise of Rights

1. A covered entity must provide individuals with a reasonable means to exercise their rights mentioned in subsections (a) and (b) in a request-form that is:—

i. clear and conspicuous;

ii. made available at no additional cost and with no transactional penalty to the individual to whom the information pertains; and

iii. in English and any other language in which the covered entity communicates with the individual to whom the information pertains.

2. A covered entity must comply with a request to exercise the rights mentioned in (a) and (b) not later than 30 days after receiving a verifiable request from the individual.

i. Where the covered entity has reasonable doubts or cannot verify the identity of the individual making a request, the covered entity may request additional personal information necessary for the specific purpose of confirming the identity of the individual.

ii. A covered entity may not de-identify an individual's personal information during the 60-day period beginning on the date on which the covered entity receives a request for correction or deletion from the individual.

Section 4. Right to know

(a) Individuals shall have the right to know what personal information a covered entity or a data processor will collect and process about the individual, including the categories and specific pieces of personal information the covered entity processes, before giving consent for the collection and processing of their personal information.

(b) Meaningful Notice. A covered entity must make both a long-form privacy policy and a short-form privacy policy available to all individuals in accordance with the following.

1. The privacy policies shall be available and readily accessible on the covered entity's website or mobile application.

i. In the case of in-person or non-internet electronic engagement, the privacy policies shall be readily accessible at the primary physical place of business and any offline equivalent maintained by the covered entity.

2. The privacy policies shall be persistently and conspicuously available at or prior to the point of sale of a product or service, subscription to a service, sign up, or creation of an account with the covered entity.

3. Covered entities that process personal information shall ensure that individuals are presented with the short-form privacy policy only once upon the individual's first electronic covered interaction that may or will result in the processing of personal information, whether that is through the covered entity's website or use of the covered entity's mobile application.

i. In the case of in-person or non-internet electronic engagement, the short-form privacy policy should be read to or otherwise presented to the individual before the covered entity first collects the individual's personal information.

4. The short-form privacy notice required under shall:—

i. be clear, concise, well-organized, and complete;

ii. be clear and prominent in appearance;

iii. use clear and plain language;

iv. use visualizations where appropriate to make complex information understandable by the ordinary user;

v. be reasonably understandable;

vi. be distinguishable from other matters;

vii. not contain any unrelated, confusing, or contradictory information;

viii. be no more than 600 words, excluding the list of third parties with which the covered entity discloses personal information; and

ix. be provided free of charge.

5. The short-form privacy notice required must include:—

i. the sensitive personal information being processed;

ii. the use model and a brief explanation of the relationship between the individual and the covered entity;

iii. whether the covered entity by itself or a data processor on its behalf processes the information;

iv. whether the covered entity uses automated decision systems;

v. whether personal information is going to be processed for purposes of targeted advertisement or monetization;

vi. one example of harm that may arise from a misuse of the personal information;

vii. the period of retention of the personal information expressed in exact dates;

viii. to what types of third parties the covered entity discloses personal information and for what purposes, including governmental entities; and

ix. whether the covered entity collects personal information through offline practices when the individual does not interact directly with the covered entity.

6. A list of the third parties referenced in (viii) must be provided either in the short-form privacy notice or in an easily accessible online form. If the policy is delivered verbally, the person communicating the policy must offer to read the list of third parties. If provided in the short-form privacy notice, such list must be offset by at least two line breaks from the rest of the short-form privacy notice.

7. The long-form privacy policy shall contain a detailed description of the processing of the personal information, including but not limited to all the elements of the short-form privacy policy, and an explanation of how the covered entities and their affiliate data processors comply with the provisions of this chapter, including the following:

i. A brief explanation of the technology that mediates the relationship between the individual and the covered entity, including automated decision systems; and

ii. A brief explanation of the risks of harm that arises from the possible misuse of personal information processing.

8. The commission shall:—

i. establish a standardized short-form privacy notice that complies with this section;

ii. determine whether a more concise presentation of a short-form privacy notice is appropriate where the policy is being communicated verbally, and if so, shall establish a standardized short-form verbal privacy notice;

iii. develop a recognizable and uniform logo or button to promote individual awareness of the short-form privacy notice; and

iv. promulgate regulations specifying additional requirements for the format and substance of short-form privacy notices.

Section 5. Right to consent

(a) Individuals shall have the right to consent in accordance with this section before their personal information is collected and processed.

(b) Consent given by an individual authorizes a covered entity to collect, cause to collect, process, or cause to process personal information from such individual in accordance with the following:

1. A covered entity must obtain consent:—

i. before collecting or causing to collect personal information for purposes of processing an individual's personal information for the first time; and

ii. after the acceptance of the short-form privacy policy described in section 4.

1. For continuing covered interactions, the consent required by this section must be renewed annually, and if not so renewed, shall be deemed to have been withdrawn.

2. A covered entity must provide new meaningful notice and obtain consent from an individual two weeks before changing the nature of the processing of personal information to which the individual previously consented.

i. The two week period in the previous paragraph shall not apply if the change in processing is necessary to enable a new functionality requested by the individual, provided that such individual was given notice and provided consent when making such request.

3. A covered entity requesting consent shall:—

i. ensure that the option to refuse consent is presented as clearly and prominently as the option to provide consent;

ii. provide a mechanism for an individual to withdraw previously given consent at any time; and

iii. once a year, provide a notice explaining how the personal information was used, including two examples of such use.

4. A covered entity requesting consent shall not coerce consent through the use of interfaces that:—

i. threaten or mandate an individual's compliance;

ii. ask questions or provide information in a way individuals cannot reasonably understand;

iii. attract the individual's attention away from their current task by exploiting perception, particularly pre-attentive processing;

iv. take advantage of individuals' errors to facilitate the interface designer's goals;

v. deliberately increase work for the individual;

vi. interrupt the individual's task flow;

vii. use information architectures and navigation mechanisms that guide the individual toward not having a real option to consent;

viii. hide desired content or interface elements;

ix. limit or omit controls that would facilitate task accomplishment by the individual;

x. present disturbing content to the individual; or

xi. generally mislead or deceive the individual.

5. Once an individual refuses to provide consent in accordance with this section, and if the individual keeps interacting with the covered entity in any way, the covered entity shall not try to obtain consent unless a period of at least six months has passed.

6. Under no circumstances shall the mere covered interaction of an individual with a covered entity's product or service be deemed as consent.

7. A covered entity may collect browser personal information, provided that the covered entity:—

i. processes only the personal information necessary to request consent;

ii. processes such information solely to request consent; and

iii. immediately deletes all the personal information if consent is refused.

1. Notwithstanding the previous paragraph, the covered entity shall retain the personal information necessary to comply with paragraph (5) of this subsection, and such information shall only be used to comply with such paragraph.

8. A covered entity shall not:—

i. refuse to serve an individual who does not approve the processing of the individual's personal information under this section unless the processing is necessary for the primary purpose of the transaction that the individual has requested;

ii. offer a program that relates the price or quality of a product or service to the degree of acceptance of personal information processing. This includes the provision of discounts or other incentives in exchange for the consent;

1. Notwithstanding the above, a covered entity may, with the individual's consent given in compliance with this section, operate a program in which information, products, or services sold to the individual are discounted based on that individual's prior purchases from the covered entity, provided that the personal information shall be processed solely to operate such program.

iii. state or imply that the quality of a product or service will be diminished and shall not actually diminish the quality of a product or service if the individual declines to give consent.

Section 6. Right to control disclosure of personal information

(a) Individuals shall have the right to (i) know the names of third parties to which the covered entities or data processors will disclose their personal information, and (ii) refuse consent for such disclosure.

(b) Disclosure of Personal Information and Relationships with Third-Parties

1. No covered entity or data processor in possession of personal information may disclose, cause to disclose, or otherwise disseminate to third parties, including government agencies, personal information unless (i) such disclosure is included in the meaningful notice pursuant to section 4, and (ii) consent from the individual is obtained in the manners and ways prescribed in section 5.

2. A covered entity shall not process or cause to process an individual's personal information acquired from a third-party, unless it has first obtained the individual's consent.

i. Notwithstanding the previous paragraph, if the processing is necessary to obtain consent, the covered entity shall:—

1. process only the personal information required to request consent;

2. process the personal information solely to request consent; and

3. immediately delete the personal information if consent is not given.

3. A covered entity shall not disclose personal information to a data processor or another third-party without a contractual agreement that:—

i. requires the data processor or third-party to meet the same privacy and security obligations as the covered entity;

ii. prohibits the data processor or third-party from processing the personal information for any purpose other than the purposes for which the individual provided consent; and

iii. prohibits the data processor or third-party from further disclosing or processing the personal information except as explicitly authorized by the contract and consistent with this chapter.

4. If a covered entity learns that a data processor or third-party to whom it has provided access to personal information is using such personal information in violation of this chapter, the covered entity shall immediately—

i. limit the violator's access to personal information;

ii. seek proof of destruction of personal information previously accessed by the violating data processor or third-party; and

iii. notify the commission about the violation.

Section 7. Prohibition of surreptitious surveillance

(a) A covered entity shall not activate the microphone, camera, or any other sensor on a device in the lawful possession of an individual that is capable of collecting or transmitting audio, video, or image data or data that can be used to measure biological or biometric information, human movement, location, chemicals, light, radiation, air pressure, speed, weight or mass, positional or physical orientation, magnetic fields, temperature, or sound without providing notice and obtaining consent pursuant to this chapter for the specific type of measurement to be activated; provided that such consent shall be effective for not more than 180 days, after which it shall expire unless renewed.

Section 8. Age of responsibility

(a) For the purposes of this chapter, individuals ages 13 and older are deemed competent to exercise all rights granted to individuals under this chapter.

(b) Rights and obligations relating to individuals under the age of 13 shall be governed by the children's online privacy protection act (15 U.S.C. Sec. 6501 et seq.) and its regulation.

Section 9. Protection of biometric and location information

(a) In addition to all provisions of this chapter generally applicable to personal information, the following provisions shall apply to the processing and collection of biometric and location information, regardless of how such biometric and location information is processed or collected:

1. Processing. No covered entity or data processor may collect or process an individual’s biometric or location information unless it first—

i. informs the individual in writing that biometric or location information is being processed and the specific purpose or purposes and length of time for which the information is being processed; and

ii. obtains consent from the individual for the specific purpose of collecting and processing biometric or location information before any such information is collected or processed.

1. For biometric information, the consent shall be handwritten and executed by the individual, explicitly authorize such processing, and be sent to the covered entity by postal mail, facsimile, or electronic scan.

2. Consent shall be for a period specified in the written consent of not more than one year and shall automatically expire at the end of such period unless renewed pursuant to the same procedures. Upon expiration of consent, any biometric or location information possessed by a covered entity must be destroyed.

3. Retention and destruction. A covered entity in possession of biometric or location information must develop a specific written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric or location information when the initial purpose for processing such information has been satisfied or within one year of the individual's consent, unless renewed, whichever occurs first.

i. Absent a valid warrant issued by a court of competent jurisdiction, a covered entity in possession of biometric or location information must comply with its established retention schedule and destruction guidelines.

4. Disclosure. No covered entity or data processor in possession of biometric or location information may disclose, cause to disclose, sell, or otherwise disseminate or cause to disseminate to third parties, including government agencies, an individual's biometric or location information unless—

i. the individual gives consent in writing to the disclosure; or

ii. the disclosure completes a financial transaction requested or authorized by the subject of the biometric or location information; or

iii. the disclosure is required by state or federal law, in which case the individual must be given adequate notice on the occasion of obtaining the consent; or

iv. the disclosure is required pursuant to a valid warrant issued by a court of competent jurisdiction, in which case the individual must be given adequate notice in accordance with section 16.

5. Monetizing. No covered entity in possession of biometric or location information may monetize or otherwise profit from an individual's biometric or location information.

i. Notwithstanding the previous paragraph, a covered entity may process an individual's biometric or location information to recommend actions, services, goods, or products provided that:—

1. there is full disclosure to the individual about the biometric or location information processed;

2. consent was given in a manner consistent with this section; and

3. there is full disclosure that such recommendation is based on the biometric or location information processed.

Section 10. Prohibition of discrimination

(a) Individuals shall have the right not to be subject to processing of their personal information that results in unlawful discriminatory actions.

(b) Covered entities that process personal information shall not engage in unlawful discriminatory practices connected with the use of personal information and the provision of services, products, or goods.

(c) Unlawful discriminatory practices are acts or practices that:—

1. process personal information in the course of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for employment, finance, healthcare, credit, insurance, housing, or education opportunities in a manner that directly results in discrimination against or otherwise makes an opportunity unavailable on the basis of an individual's or group of individuals' actual or perceived belonging to a protected class under section 4 of chapter 151B;

2. process personal information in a manner that discriminates in, or otherwise makes unavailable, whether in a commercial transaction or otherwise, any place of public accommodation, resort, or amusement as defined in section 92A of chapter 272, on the basis of an individual's or group of individuals' actual or perceived belonging to a protected class under section 4 of chapter 151B; or

3. enable the use of covered entities' services or products to place targeted advertisements for employment, finance, healthcare, credit, insurance, housing, or education opportunities in such a way that enables the advertiser to determine whether to serve an ad to an individual or group of individuals on the basis of actual or perceived belonging to a protected class under section 4 of chapter 151B.

(d) Nothing in this section shall limit covered entities from processing personal information for:

1. legitimate testing to prevent unlawful discrimination or otherwise determine the extent or effectiveness of the covered entity's compliance with this section; and

2. the purpose of advertising, marketing, soliciting, or offering education or employment opportunities to members of a protected class under section 4 of chapter 151B so

long as such opportunities are within an affirmative action, diversity program, or similar initiative that intends to provide opportunities to the protected classes.

Section 11. Prohibition of unfair and deceptive trade practices

(a) Covered entities that process personal information shall be subject to chapter 93A in connection with the use of personal information and the provision of services, products, or goods.

(b) Unfair and deceptive trade practices are acts or practices that:-

1. materially interfere with the ability of an individual to understand the way the covered entity processes personal information; or

2. take unreasonable advantage of:—

i. a lack of understanding on the part of the individual of the material risks, costs, or conditions of the processing of personal information; or

ii. the inability of the individual to protect the interests of the individual in selecting or using a product, good, or service provided by the covered entity; or

iii. the reasonable reliance by the individual on a covered entity to act in the interests of the consumer.

Section 12. The Massachusetts information privacy commission

(a) The commission shall have all the powers necessary or convenient to carry out and effectuate its purposes including, but not limited to, the power to:—

1. appoint officers and hire employees;

2. establish and amend a plan of organization that it considers expedient;

3. execute all instruments necessary or convenient for accomplishing the purposes of this chapter and its regulation;

4. adopt, amend, or repeal regulations for the implementation, administration, and enforcement of this chapter.

5. enter into agreements or other transactions with a person, including, but not limited to, a governmental entity or other governmental instrumentality or authority in connection with its powers and duties under this chapter;

6. appear on its own behalf before boards, commissions, departments, or other agencies of municipal, state, or federal government;

7. apply for and accept subventions, grants, loans, advances, and contributions of money, property, labor, or other things of value from any source, to be held, used, and applied for its purposes;

8. provide and pay for advisory services and technical assistance as may be necessary for its judgment to carry out this chapter and fix the compensation of persons providing such services or assistance;

9. prepare, publish and distribute, with or without charge as the commission may determine, such studies, reports, bulletins, and other materials as the commission considers appropriate;

10. gather facts and information applicable to the commission's obligation to enforce this chapter and ensure its compliance;

11. conduct investigations for possible violations of this chapter;

12. conduct adjudicatory proceedings and promulgate regulations in accordance with chapter 30A;

13. refer cases for criminal prosecution to the appropriate federal, state, or local authorities;

14. maintain an official internet website for the commission.

15. conduct a study to determine the most effective way for covered entities to obtain individuals' consent in accordance with section 5 for each type of personal information processing.

i. The commission may request data and information from covered entities conducting business in Massachusetts, Massachusetts government entities administering notice and consent regimes, consumer protection experts, privacy advocates, and researchers, Internet standards-setting bodies such as the Internet Engineering Taskforce and Institute of Electrical and Electronics Engineers, and other relevant sources to meet the purpose of the study.

16. assess and impose civil administrative penalties on covered entities, data processors, and third parties who fail to comply with or violate any provision of this chapter or regulation enacted pursuant to this chapter, and create an administrative procedure for such purpose.; and

17. create and disseminate information to the public about their rights in relation to personal information privacy and what to do if they believe their rights have been violated.

Section 13. Enforcement – Civil administrative penalties.

(a) Any individual or group of individuals alleging a violation of this chapter or a regulation promulgated under this chapter may bring an administrative complaint before the commission.

1. The commission shall promulgate a form of complaint for use under this section, which shall be in such form and language to permit an individual to prepare and file such complaint pro se.

2. An individual shall not be required to accept mandatory arbitration of a claim under this chapter as a condition of bringing an administrative complaint.

3. The administrative complaint shall be directed against the covered entity, data processor, and the third-parties alleged to have committed the violation.

4. The commission shall investigate the allegations and decide whether it amounts to the imposition of a civil administrative penalty.

(b) The commission shall also open investigations without any particular alleged violation to assess the compliance of covered entities, data processors, and third parties with this chapter and shall impose civil administrative penalties if necessary.

(c) Whenever the commission seeks to assess a civil administrative penalty on any covered entities, data processors, and third parties, the commission shall cause to be served upon such person, either by service, in hand, or by certified mail, return receipt requested, a written

notice of its intent to assess a civil administrative penalty which shall include: a concise statement of the alleged act or omission for which such civil administrative penalty is sought to be assessed, each law, regulation, or order violated as a result of such alleged act or omission; the amount which the commission seeks to assess as a civil administrative penalty for each such alleged act or omission; a statement of such person's right to an adjudicatory hearing on the proposed assessment; the requirements such person must comply with to avoid being deemed to have waived the right to an adjudicatory hearing; and the manner of payment thereof if such person elects to pay the penalty and waive an adjudicatory hearing. After such notice of intent to assess a civil administrative penalty has been given, each such day thereafter during which such noncompliance or violation occurs or continues shall constitute a separate offense and shall be subject to a separate civil administrative penalty if reasonable efforts have not been made to promptly come into compliance.

(d) Whenever the commission seeks to assess a civil administrative penalty on any person, such person shall have the right to an adjudicatory hearing under chapter 30A, whose provisions shall apply except when they are inconsistent with the provisions of this section. Such person shall be deemed to have waived such right to an adjudicatory hearing unless, within twenty-one days of the date of the commission's notice of intent to assess a civil administrative penalty, such person files with the commission a written statement denying the occurrence of any of the acts or omissions alleged by the commission in such notice, or asserting that the money amount of the proposed civil administrative penalty is excessive. In any adjudicatory hearing authorized pursuant to chapter 30A, the commission shall, by a preponderance of the evidence, prove the occurrence of each act or omission alleged by the commission.

(e) If a person waives his right to an adjudicatory hearing, the proposed civil administrative penalty shall be final immediately upon such waiver.

(f) If a civil administrative penalty is assessed at the conclusion of an adjudicatory hearing, said civil administrative penalty shall be final upon the expiration of thirty days if no action for judicial review of such decision is commenced pursuant to chapter 30A.

(g) Any person who institutes proceedings for judicial review under chapter 30A of the final assessment of a civil administrative penalty shall place the full amount of the final assessment in an interest-bearing escrow account in the custody of the clerk/magistrate of the reviewing court. The establishment of such an interest-bearing escrow account shall be a condition precedent to the jurisdiction of the reviewing court unless the party seeking judicial review demonstrates in a preliminary hearing held within twenty days of the filing of the complaint either the presence of a substantial question for review by the court or an inability to pay. Upon such a demonstration, the court may grant an extension or waiver of the interest-bearing escrow account or may require, in lieu of such interest-bearing escrow account, the posting of a bond payable directly to the commonwealth in the amount of one hundred and twenty-five percent of the assessed penalty. If, after judicial review, in a case where the requirement for an escrow account has been waived, and in cases where a bond has been posted in lieu of such requirement, the court affirms, in whole or in part, the assessment of a civil administrative penalty the commission shall be paid the amount thereof together with interest at the rate set forth in section six C of chapter two hundred and thirty-one. If, after such review in a case where an interest-bearing escrow account has been established, the court affirms the assessment of such penalty, in whole or in part, the commission shall be paid the amount thereof together with the accumulated interest thereon in such interest-bearing escrow account. If the

court sets aside the assessment of a civil administrative penalty in a case where the amount of such penalty has been deposited in an interest-bearing escrow account, the person on whom the civil administrative penalty was assessed shall be repaid the amount so set aside, together with the accumulated interest thereon.

(h) Each person who fails to pay a civil administrative penalty on time, and each person who issues a bond pursuant to this section and who fails to pay to the commonwealth on time the amount required hereunder, shall be liable to the commonwealth for up to three times the amount of the civil administrative penalty, together with costs, plus interest from the time the civil administrative penalty became final and attorneys' fees, including all costs and attorneys' fees incurred directly in the collection thereof. The rate of interest shall be the rate set forth in section 6C of chapter 231.

(i) No civil administrative penalty assessed hereunder shall be:

1. less than 0.15% of the annual global revenue of the covered entity, data processor, or third-party or $15,000, whichever is greater, per individual violation; or

2. more than 4% of the covered entity's annual global revenue, data processor, or third-party or $20,000,000, whichever is greater, if the commission assesses a civil administrative penalty for multiple violations that affect multiple individuals.

(j) In determining the amount of each civil administrative penalty, the commission shall include, but not be limited to, the following in its consideration:—

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;

(k) Notwithstanding any general or special law to the contrary, including the limitations and considerations set forth in this section, the commission may require that the amount of a civil administrative penalty imposed pursuant to this section exceeds the economic benefit realized by a person for noncompliance.

(l) When imposing civil administrative penalties, the commission shall consider the following:—

1. each individual whose personal information was unlawfully processed, and each instance of processing counts as a separate violation;

2. each paragraph of this chapter that was violated counts as a separate violation;

3. if a series of steps or transactions were component parts of a single transaction to avoid the reach of this chapter, the commission shall disregard the intermediate steps or transactions and consider everything one transaction.

(m) All civil administrative penalties assessed shall be paid to the commonwealth. Once the payment is received, the commonwealth shall:—

1. earmark 10% of the civil administrative penalties collected to fund the commission's budget; and

2. identify the individuals affected by the violation and use the remaining proceeds collected to redress and mitigate harms caused by the violation.

Section 14. Enforcement - Judicial remedies

(a) Private right of action. Any individual alleging a violation of this chapter or a regulation promulgated under this chapter may bring a civil action in any court of competent jurisdiction.

1. 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.

2. The civil action shall be directed to the covered entity, data processor, and the third-parties alleged to have committed the violation.

3. A violation of this chapter or a regulation promulgated under this chapter regarding an individual's personal information constitutes a rebuttable presumption of harm to that individual.

4. In a civil action in which the plaintiff prevails, the court may award:—

i. 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;

ii. punitive damages; and

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

5. 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.

6. The court may request the opinion of the commission on the matters discussed.

(b) The attorney general may bring an action pursuant to section 4 of chapter 93A against a covered entity, data processor, or third-party 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, act, 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. During the proceedings, the court may also request the opinion of the commission on the matters discussed.

3. 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.

(c) When calculating awards and civil penalties in all the actions in this section, a court shall consider the factors mentioned in subsection (j) of section 13.

(d) When assessing the defendant's behavior in judicial proceedings, the court shall consider the factors mentioned in subsection (l) of section 13.

(e) 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) Non-waivable rights. 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 4 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. § 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. § 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. Exceptions

(a) A covered entity shall not be required to provide meaningful notice or obtain consent for processing personal information in accordance with sections 4 and 5 when:—

1. the processing is necessary to execute the specific transaction for which the individual is providing personal information, such as the provision of financial information to complete a purchase or the provision of a mailing address to deliver a package;

i. Notwithstanding the previous paragraph, personal information shall not be processed for any other purpose beyond that clear primary purpose without providing meaningful notice to and obtaining consent from the individual to whom the personal information pertains.

2. the covered entity believes that (i) an emergency involving immediate danger of death or serious physical injury to any individual requires obtaining without delay personal

information so that it can be used to respond to the emergency, and (ii) the request is narrowly tailored to address the emergency, subject to the following limitations.

i. The request shall document the factual basis for believing that an emergency involving immediate danger of death or serious physical injury to an individual requires obtaining without delay personal information relating to the emergency; and

ii. Simultaneous with the covered entity obtaining personal information under this paragraph, the covered entity shall use reasonable efforts to inform the individual of the personal information obtained; the details of the emergency; and the reasons why the covered entity needed to obtain the personal information and shall continue such efforts to inform until receipt of information is confirmed; or

3. the processing involves only de-identified information, provided that a covered entity that processes de-identified information must—

i. have a privacy policy that details how the de-identified information is processed;

ii. implement technical safeguards that prohibit indirect re-identification of the information;

iii. implement business processes that expressly prohibit indirect re-identification of the information;

iv. implement business processes that prevent inadvertent release of de-identified information; and

v. not attempt to re-identify the information.

(b) A covered entity, its affiliated data processors, or the third parties they contracted with shall not be required to obtain consent for disclosing or sharing personal information in accordance with this chapter if:—

1. Disclosure is required to respond to a legal request, provided that—

i. a covered entity receiving such legal request shall serve or deliver the following information to the individual to which the legal request for personal information refers by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective:—

1. A copy of the legal request and a notice that informs the individual of the nature of the inquiry with reasonable specificity;

2. That personal information related to the individual was supplied to, or requested by, a requesting entity and the date on which the supplying or request took place;

3. An inventory of the personal information requested or supplied;

4. Whether the information was in possession of the covered entity, an affiliate data processor, or a third-party they contracted with; and

5. The identity of the person that sought the legal request from the court, if known.

ii. The covered entity shall serve or deliver such notification immediately upon receiving a legal request asking for or compelling the disclosure of personal information, provided that a covered entity may apply to the court for an order delaying notification. The court may issue the order if notification of the existence of the legal request will result in danger to the life or physical safety of an individual, flight from prosecution, destruction of or tampering

with evidence, or intimidation of potential witnesses, or otherwise seriously jeopardize an investigation or unduly delay a trial.

1. If granted, such an order shall not exceed 30 days but may be renewed up to 30 days at a time while grounds for the delay persist.

2. The disclosure is a routine disclosure required by state or federal law, provided that the individual received notice of such requirement in accordance with sections 4 and 6.

Section 17. 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 commission 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; and

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;

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;

2. 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

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

(b) Covered entities that are required to disclose personal information as a matter of law pursuant to section 16(b)(2) shall provide the commission and the general public a bi-monthly report containing the following aggregate information:—

1. The total number of times that they share information, disaggregated by:—

i. applicable law or statute that mandates such disclosure;

ii. government entity or private party that received the information; and

iii. the type of personal information disclosed.

2. The total number of individuals affected by such disclosures, disaggregated by race, ethnicity, gender, and age, if such demographics are known.

(c) The commission shall:—

1. establish a standardized reporting form to comply with this section;

2. determine whether a more concise presentation of the reporting is appropriate and, if so, shall establish a standardized version of such form;

3. dedicate a section of its website to making the reports available to the general public; and

4. promulgate regulations specifying additional requirements for purposes of advancing information related to the sharing of information with the government.

Section 18. 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 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. 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.

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 19. Relationship with other laws

(a) The provisions of this chapter shall supersede local or state laws, regulations, and ordinances, except when such local or state laws, regulations, or ordinances provide stronger privacy protections for individuals.

(b) This chapter covers businesses that are subject to federal laws concerning the processing of individuals' personal information to the extent that (i) this chapter provides stronger privacy protections for individuals than those federal laws; and (ii) those federal laws do not explicitly preempt state laws.

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

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 10 of the General Laws, as appearing in the 2018 Official Edition, is hereby amended by inserting after section 78 the following sections:-

Section 79.

(a) There shall be a Massachusetts information privacy commission to have general supervision and sole regulatory and enforcement authority over chapter 93L of the General Laws.

(b) The commission shall consist of 5 commissioners: 1 of whom shall be appointed by the governor; 1 of whom shall be appointed by the attorney general; 1 of whom shall be appointed by the secretary of the commonwealth; and 2 of whom shall be appointed by a majority vote of the governor, attorney general and secretary of the commonwealth. The secretary of the commonwealth shall designate the chair of the commission. The chair shall serve in that capacity throughout the term of appointment and until a successor shall be appointed.

(c) All commissioners must have a background in one or more of the following:—

1. information privacy, technology, and the law;

2. social implications of artificial intelligence and digital equity;

3. data science and data surveillance; or

4. digital services, digital markets, and consumer protection of digital data.

(d) Prior to appointment to the commission, a background investigation shall be conducted into the financial stability, integrity, and responsibility of a candidate, including the candidate's reputation for good character and honesty.

(e) Each commissioner shall be a resident of the commonwealth within 90 days of appointment and, while serving on the commission, shall not: (i) hold, or be a candidate for, federal, state, or local elected office; (ii) hold an appointed office in a federal, state or local government; or (iii) serve as an official in a political party. Not more than three commissioners shall be from the same political party.

(f) Each commissioner shall serve for a term of 5 years or until a successor is appointed and shall be eligible for reappointment; provided, however, that no commissioner shall serve more than 10 years. A person appointed to fill a vacancy in the office of a commissioner shall be appointed in a like manner and shall serve for only the unexpired term of that commissioner.

(g) The secretary of the commonwealth, the governor or the attorney general may remove a commissioner who was appointed by that appointing authority if the commissioner: (i) is guilty of malfeasance in office; (ii) substantially neglects the duties of a commissioner; (iii) is unable to discharge the powers and duties of the office; (iv) commits gross misconduct; or (v) is convicted of a felony. The secretary of the commonwealth, the governor and the attorney general may, by majority vote, remove a commissioner who was appointed by a majority vote of the secretary of the commonwealth, the governor and the attorney general if the commissioner: (i) is guilty of malfeasance in office; (ii) substantially neglects the duties of a commissioner; (iii) is unable to discharge the powers and duties of the commissioner's office; (iv) commits gross

misconduct; or (v) is convicted of a felony. Before removal, the commissioner shall be provided with a written statement of the reason for removal and an opportunity to be heard.

(h) Three commissioners shall constitute a quorum, and the affirmative vote of 3 commissioners shall be required for an action of the commission. The chair or 3 members of the commission may call a meeting; provided, however, that notice of all meetings shall be given to each commissioner and to other persons who request such notice. The commission shall adopt regulations establishing procedures, which may include electronic communications, by which a request to receive notice shall be made and the method by which timely notice may be given.

(i) Commissioners shall receive salaries not greater than ¾ of the salary of the secretary of administration and finance under section 4 of chapter 7; provided, however, that the chair shall receive a salary equal to the salary of the secretary of administration and finance. Commissioners shall devote their full time and attention to the duties of their office.

(j) The commission shall annually elect 1 of its members to serve as secretary and 1 of its members to serve as treasurer. The secretary shall keep a record of the proceedings of the commission and shall be the custodian and keeper of the records of all books, documents, and papers filed by the commission and of its minute book. The secretary shall cause copies to be made of all minutes and other records and documents of the commission and shall certify that such copies are true copies, and all persons dealing with the commission may rely upon such certification.

(k) The chair shall have and exercise supervision and control over all the affairs of the commission. The chair shall preside at all hearings at which the chair is present and shall designate a commissioner to act as chair in the chair's absence. To promote efficiency in

administration, the chair shall make such division or re-division of the work of the commission among the commissioners as the chair deems expedient.

(l) The commissioners shall, if so directed by the chair, participate in the hearing and decision of any matter before the commission; provided, however, that at least 2 commissioners shall participate in the hearing and decision of matters other than those of formal or administrative character coming before the commission; and provided further, that any such matter may be heard, examined and investigated by an employee of the commission designated and assigned by the chair, with the concurrence of 1 other commissioner. Such employee shall make a report in writing relative to the hearing, examination, and investigation of every such matter to the commission for its decision. For the purposes of hearing, examining, and investigating any such matter, such employee shall have all of the powers conferred upon a commissioner by this section. For each hearing, the concurrence of a majority of the commissioners participating in the decision shall be necessary.

(m) The commission shall appoint an executive director. The executive director shall serve at the pleasure of the commission, shall receive such salary as may be determined by the commission, and shall devote full time and attention to the duties of the office. The executive director shall be a person with skill and experience in management, shall be the executive and administrative head of the commission, and shall be responsible for administering and enforcing the law relative to the commission and each administrative unit thereof. The executive director shall appoint and employ a chief financial and accounting officer and may, subject to the approval of the commission, employ other employees, consultants, agents, and advisors, including legal counsel, and shall attend meetings of the commission. The chief financial and accounting officer of the commission shall be in charge of its funds, books of account, and

accounting records. No funds shall be transferred by the commission without the approval of the commission and the signatures of the chief financial and accounting officer and the treasurer of the commission. In the case of an absence or vacancy in the office of the executive director or in the case of disability, as determined by the commission, the commission may designate an acting executive director to serve as executive director until the vacancy is filled or the absence or disability ceases. The acting executive director shall have all of the powers and duties of the executive director and shall have similar qualifications as the executive director.

(n) Chapters 268A and 268B shall apply to the commissioners and to employees of the commission; provided, however, that the commission shall establish a code of ethics for all members and employees that shall be more restrictive than said chapters 268A and 268B. A copy of the code shall be filed with the state ethics commission. The code shall include provisions reasonably necessary to carry out the purposes of this section and any other laws subject to the jurisdiction of the commission including, but not limited to: (i) prohibiting the receipt of gifts by commissioners and employees from any entity subject to the jurisdiction of the commission; (ii) prohibiting the participation by commissioners and employees in a particular matter as defined in section 1 of said chapter 268A that affects the financial interest of a relative within the third degree of consanguinity or a person with whom such commissioner or employee has a significant relationship as defined in the code; and (iii) providing for recusal of a commissioner in a decision due to a potential conflict of interest.

(o) The Massachusetts information privacy commission shall be a commission for the purposes of section 3 of chapter 12.

(p) The commission shall, for the purposes of compliance with state finance law, operate as a state agency as defined in section 1 of chapter 29 and shall be subject to the laws applicable to agencies under the control of the governor; provided, however, that the comptroller may identify any additional instructions or actions necessary for the commission to manage fiscal operations in the state accounting system and meet statewide and other governmental accounting and audit standards. The commission shall properly classify the commission's operating and capital expenditures and shall not include any salaries of employees in the commission's capital expenditures. Unless otherwise exempted by law or the applicable central service agency, the commission shall participate in any other available commonwealth central services including, but not limited to, the state payroll system pursuant to section 31 of said chapter 29, and may purchase other goods and services provided by state agencies in accordance with comptroller provisions. The comptroller may chargeback the commission for the transition and ongoing costs for participation in the state accounting and payroll systems and may retain and expend such costs without further appropriation for the purposes of this section. The commission shall be subject to section 5D and subsection (f) of section 6B of said chapter 29.

(q) The commission shall be subject to chapter 30A.

Section 80.

(a) There shall be an information privacy advisory board to study and make recommendations to the Massachusetts information privacy commission on issues related to information privacy in the Commonwealth. The board shall consist of: the executive director of the Massachusetts information privacy commission who shall serve as chair; the secretary of technology services and security or the secretary's designee; the house and senate chairs of the

joint committee on state administration and regulatory oversight; the chief justice of the supreme judicial court or a designee; the attorney general or a designee; the state auditor or a designee; the inspector general or a designee; the secretaries of the executive office of public safety and security, department of children and families, and executive office of health and human services, or their designees; the chief counsel of the committee for public counsel services or a designee; the chief legal counsel of the Massachusetts Bar Association or a designee; the executive director of the American Civil Liberties Union of Massachusetts or a designee; 2 academics who shall be experts in (i) data science, artificial intelligence, and machine learning, (ii) social implications of artificial intelligence and technology, or (iii) information policy, technology, and the law; 2 academics who shall be experts in (i) artificial intelligence and machine learning, (ii) data science and information policy, or (iii) technology and the law; the executive director of the Massachusetts Law Reform Institute or a designee; 1 representative from a the National Association of Social Workers; and 1 representative from the Massachusetts High Technology Council. Members of the board shall serve for terms of 2 years. Members of the board shall serve without compensation but shall be reimbursed for their expenses actually and necessarily incurred in the discharge of their official duties. Members of the board shall not be state employees under chapter 268A by virtue of their service on the board. To take action at a meeting, a majority of the members of the board present and voting shall constitute a quorum.

(b) The information privacy advisory board shall: (i) consider all matters submitted to it by the commission; (ii) on its own initiative, recommend to the commission guidelines, rules and regulations and any changes to guidelines, rules, and regulations that the advisory board considers important or necessary for the commission’s review and consideration; and (iii) advise on the preparation of regulations pursuant to chapter 93L of the general laws.

(c) The chair may appoint subcommittees to expedite the work of the board.

SECTION 3. Section 5 of Chapter 93H of the General Laws, as appearing in the 2020 Official Edition, is hereby amended by inserting after the words “office of consumer affairs and business regulation” in the two places where those words appear the following:

, and the Massachusetts information privacy commission

SECTION 4. 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:

“Information” also referred to as “employee information,” or “data” means 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.

“Electronic monitoring” means the collection of information concerning employee activities, communications, actions, biometrics, or behaviors by electronic means.

“Employment-related decision” means 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.

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

"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 5. Effective date

(a) Section 2 shall take effect immediately.

(b) The remaining sections shall take effect 12 months after this Act is enacted.

(c) The enforcement of chapter 93L shall be delayed until 18 months after this Act is enacted.