HOUSE DOCKET, NO. 3847 FILED ON: 2/19/2021

# HOUSE . . . . . No. 136

The Commonwealth of Massachusetts

PRESENTED BY:

***David M. Rogers and Andres X. Vargas***

*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 relative to data privacy.

PETITION OF:

| NAME: | DISTRICT/ADDRESS: | DATE ADDED: |
|---|---|---|
| *David M. Rogers* | *24th Middlesex* | *2/19/2021* |
| *Andres X. Vargas* | *3rd Essex* | *2/21/2021* |
| *Patrick Joseph Kearney* | *4th Plymouth* | *2/22/2021* |
| *Kate Lipper-Garabedian* | *32nd Middlesex* | *2/26/2021* |
| *David Henry Argosky LeBoeuf* | *17th Worcester* | *2/26/2021* |
| *Lindsay N. Sabadosa* | *1st Hampshire* | *2/26/2021* |
| *Dylan A. Fernandes* | *Barnstable, Dukes and Nantucket* | *3/8/2021* |
| *Bradley H. Jones, Jr.* | *20th Middlesex* | *3/9/2021* |
| *Elizabeth A. Malia* | *11th Suffolk* | *3/15/2021* |
| *David Allen Robertson* | *19th Middlesex* | *3/16/2021* |
| *Jessica Ann Giannino* | *16th Suffolk* | *11/16/2021* |

HOUSE DOCKET, NO. 3847 FILED ON: 2/19/2021

# HOUSE . . . . . No. 136

By Messrs. Rogers of Cambridge and Vargas of Haverhill, a petition (accompanied by bill, House, No. 136) of David M. Rogers, Andres X. Vargas and others relative to data privacy. Advanced Information Technology, the Internet and Cybersecurity.

## The Commonwealth of Massachusetts

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

An Act relative to data privacy.

*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 are hereby amended by inserting after chapter 93K the following chapter:-

CHAPTER 93L. Data Accountability and Transparency Agency.

Section 1. Definitions.

For purpose of this chapter, the following words and terms shall have the following meanings:

“Affiliate”, means any person that controls, is controlled by, or is under common control with another person.

“Agency”, means the Massachusetts Data Accountability and Transparency Agency established in section 5.

"Anonymized Data", means information that has been proven to not identify, relate to, describe, reference, be capable of being associated with, or be linked or reasonably linkable to a particular individual or device.

"Automated Decision System", means a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision, or facilitates human decision-making.

"Automated decision system impact evaluation", means a study conducted after deployment of an automated decision system that includes, at a minimum—(a) an evaluation of an automated decision system's accuracy, bias on the basis of protected class, and impact on privacy on individuals or groups of individuals; (b) an evaluation of the effectiveness of measures taken to minimize risks as outlined in any prior automated decision system risk assessments; and (c) recommended measures to further minimize risks to accuracy, bias on the basis of protected class, and privacy on individuals or groups of individuals.

"Automated decision system risk assessment", means a study evaluating an automated decision system and the automated decision system's development process, including the design and training data of the automated decision system, for potential risks to accuracy, bias, discrimination, and privacy on individuals or groups of individuals that includes, at a minimum—(a) a detailed description of the automated decision system, including—(i) its design and methodologies; (ii) training data characteristics; (iii) data; and (iv) purpose; (b) an assessment of the automated decision system governance in light of its purpose, potential unintended consequences, and taking into account relevant factors, including—(i) the duration and methods for which personal data and the results of the automated decision system are stored;

(ii) what information about the automated decision system (including inputs, features, and results) is available to individuals; and (iii) the recipients of the results of the automated decision system; (c) an assessment of the risks posed by the automated decision system—(i) poses to individuals or groups of individuals of privacy harm; and (ii) may result in or contribute to in accurate, biased, or discriminatory decisions impacting individuals or groups of individuals; (D) the measures a data aggregator will employ to minimize the risks described in subparagraph (C), including technological and physical safeguards.

"Collect", (a) means buying, renting, gathering, obtaining, receiving, or accessing any personal data by any means; and (b) includes—(i) receiving personal data from an individual or device; and (ii) creating, deriving, or inferring personal data by observing the behavior of an individual.

"Commissioner," means the Commissioner of the Massachusetts Data Accountability and Transparency Agency.

"Covered individual", means an applicant, current or former employee, contractor, subcontractor, grantee, or agent of a data aggregator or service provider.

"Data Aggregator", means (a) any person that collects, uses, or shares an amount of personal data that is not de minimis; and (b) does not include an individual who collects, uses, or shares personal data solely for personal reasons.

"Device", means any physical object that— (a) is capable of connecting to the internet or other communication network; or (b) has computer processing capabilities that can collect, send, receive, or store data.

"Electronic data", means any information that is in an electronic or digital format or any electronic or digital reference that contains information about an individual or device.

"Facial recognition technology", means an automated or semiautomated process that assists in identifying or verifying an individual based on the characteristics of the face of an individual.

"Individual", means a natural person.

"Intentional interaction", means an interaction in which an individual engages in 1 or more actions to demonstrate that the individual intends to interact with a data aggregator.

"Journalism", means the gathering, preparing, collecting, photographing, recording, writing, editing, reporting, or publishing of news or information that concerns local, national, or international events or other matters of public interest for dissemination to the public; and includes the collection or use of personal data about a public individual or official, or that otherwise concerns matters of public interest, for dissemination to the public.

"Person", means an individual, a local, State, or Federal governmental entity, a partnership, a company, a corporation, an association (incorporated or unincorporated), a trust, an estate, a cooperative organization, another entity, or any other organization or group of such entities acting in concert.

"Personal data", means electronic data that, alone or in combination with other data—(A) could be linked or reasonably linkable to an individual, household, or device; or (B) could be used to determine that an individual or household is part of a protected class.

''Privacy harm'' means an adverse consequence, or a potential adverse consequence, to an individual, a group of individuals, or society caused, or potentially caused, in whole or in part, by the collection, use, or sharing of personal data, including—(a) direct or indirect financial loss or economic harm, including financial loss or economic harm arising from fraudulent activities or data security breaches; (b) physical harm, harassment, or a threat to an individual or property; (c) psychological harm, including anxiety, embarrassment, fear, other trauma, stigmatization, reputational harm, or the revealing or exposing of an individual, or a characteristic of an individual, in an unexpected way; (d) an adverse outcome or decision, including relating to the eligibility of an individual for the rights, benefits, or privileges in credit and insurance (including the denial of an application or obtaining less favorable terms), housing, education, professional certification, employment (including hiring, firing, promotion, demotion, and compensation), or the provision of health care and related services; (e) discrimination or the otherwise unfair or unethical differential treatment with respect to an individual, including in a manner that is prohibited under Section 9 of this chapter; (f) the interference with, or the surveillance of, activities that are protected by the First Amendment to the Constitution of the United States; (g) the chilling of free expression or action of an individual, or society generally, due to perceived or actual pervasive and excessive collection, use, or sharing of personal data; (h) the impairment of the autonomy of an individual or society generally; and (i) any harm fairly traceable to an invasion of privacy tort; and (j) any other adverse consequence, or potential adverse consequence, consistent with the provisions of this Act, as determined by the Director.

"Protected class", means the actual or perceived race, color, ethnicity, national origin, religion, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability of an individual or a group of individuals.

“Public accommodation’’ means any type of business considered a place of public accommodation pursuant to section 201(b) of the Civil Rights Act of 1964 (42 U.S.C. 2000a(b)) or section 301(7) of the Americans with Disabilities Act of 1990 (42 U.S.C. 12181(7)) or a business that offers goods or services through the internet to the general public.

“Service provider”, means a data aggregator that collects, uses, or shares personal data only on behalf of another data aggregator in order to carry out a permissible purpose.

“Share”, means disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, personal data, except for as required under section 9 of this chapter.

“Use”, means to perform an operation or a set of operations on personal data, either manually or by automated means, after the collection of the data, including—(a) the analysis, organization, storage, retention, or maintenance of the data; and (b) the derivation or inference of information from the personal data.

“Verifiable request”, means a request that a data aggregator can reasonably verify is made—(a) by an individual; (b) by an individual on behalf of the individual’s minor child; or (c) by a person registered with the Secretary of State authorized by the individual to act on the individual’s behalf.

Section 2. Massachusetts Data Accountability and Transparency Agency.

(a) There shall be a Massachusetts Data Accountability and Transparency Agency which shall consist of one commissioner who shall exercise supervision and control over the agency, whom shall be appointed by a majority vote of the treasurer and receiver-general, the governor,

and the attorney general and shall have a background in technology; protection of personal data; civil rights and liberties; law; social sciences; and business.

(b) The commissioner shall serve in that capacity for a term of five years and until a successor shall be appointed. The commissioner shall be eligible for reappointment; provided, however that no commissioner shall serve more than 10 years. An individual appointed to fill the vacancy of commissioner shall be appointed in a like manner.

(c) The commissioner shall be a resident of the commonwealth within 90 days of appointment and, while serving as commissioner, 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. The commissioner shall receive a salary equal to the salary of the secretary of administration and finance under section 4 of chapter 7. The commissioner shall devote their full time and attention to the duties of their office and shall hold no other employment.

(d) The treasurer and receiver-general, the governor, and the attorney general may remove the commissioner, by a majority vote, 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. Before removal, the commissioner shall be provided with a written statement of the reason for removal and shall have an opportunity to be heard.

(e) The commissioner, through the agency, shall have all the powers necessary or convenient to carry out and effectuate its purposes including, but not limited to, the power to: (i) appoint officers, hire employees and make such divisions or other offices among employees of

the agency; (ii) establish and amend a plan of organization that it considers expedient; (iii) execute all instruments necessary or convenient for accomplishing the purposes of this chapter; (iv) enter into agreements or other transactions with a person, including, but not limited to, a public entity or other governmental instrumentality or authority in connection with its powers and duties under this chapter; (v) appear on its own behalf before boards, commissions, departments or other agencies of municipal, state or federal government; (vi) 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; (vii) provide and pay for advisory services and technical assistance as may be necessary in its judgment to carry out this chapter and fix the compensation of persons providing such services or assistance; (viii) prepare, publish and distribute, with or without charge as the commissioner may determine, such studies, reports, bulletins and other materials as the commissioner considers appropriate; (ix) gather facts and information applicable to the agency's obligations; (x) conduct investigations into covered entities, including data aggregators and service providers; (xi) impose fees and fines, as authorized by this chapter and penalties and sanctions for a violation of this chapter or any regulations promulgated by the agency; (xii) collect fees under this chapter; (xiii) conduct adjudicatory proceedings and promulgate regulations in accordance with chapter 30A and may adopt regulations and establish procedures that include electronic communications, by which a request to receive notice shall be made and the method by which timely notice may be given; (xiv) refer cases for criminal prosecution to the appropriate federal, state or local authorities; (xv) maintain an official internet website for the agency; (xvi) monitor any federal activity regarding data privacy; (xvii) delegate to any employee, representative, or agent any powers vested in the agency by law; (xviii) adopt and use a seal; (xix) use and expend funds; (xx) implement this

chapter through orders, guidance documents, interpretations, statements of policy, examinations, investigations, joint investigations, and enforcement actions; (xxi) monitor risks to individuals or groups of individuals in collection, use, and sharing of personal data and report risks to the public; and (xxii) perform such other functions as may be authorized or required by law.

(f) The commissioner shall file an annual report with the secretary of the executive office of administration and finance, the clerks of the senate and the house of representatives, and the senate and house committees on ways and means: (i) listing the number of employees of the agency, the salaries and titles of each employee, the source of funding for the salaries of said employees and the projected date when federal funds for such positions are expected to terminate; (ii) listing and describing grant programs of the department funded by the federal government, including the amount of funding by grant; (iii) listing and describing other programs of the agency; and (iv) any other amounts to be spent by category and grantee. Such reports shall be filed annually on or before December thirty-first and shall refer to activities planned for the subsequent calendar year. The commissioner shall also file with said committees an annual report detailing all expenditures in the agency by the division, identified by categories of projects and grantees under each category, together with all available documentation resulting from such expenditures. Such reports shall be filed on or before March first of each year and shall refer to activities in the preceding calendar year.

(g) The commissioner shall be sworn to the faithful performance of their official duties. The commissioner shall not own, or be in the employ of, or own any stock in any data aggregator or data service provider nor shall they be in any way directly or indirectly pecuniarily interested in or connected with any such company or in the employ or connected with any person financing any such company. The commissioner shall not personally or through any partner or agent render

any professional service or make or perform any business contract with or for any data aggregator or data service provider, nor shall the commissioner directly or indirectly receive any commission, bonus, discount, present, or reward from any such company.

(h) The commissioner shall appoint an executive director. The executive director shall serve at the pleasure of the commissioner and shall receive ¾ the salary of the commissioner, and shall devote full time and attention to the duties of the office and shall hold no other employment during their period of service. The executive director shall be a person with skill and experience in management, shall be the executive and administrative head of the agency and shall be responsible for administering and enforcing the law relative to the agency and to each administrative unit thereof. With the consent of the commissioner, the executive director shall appoint and employ a chief financial and accounting officer and may, employ other employees, consultants, agents and advisors, including legal counsel. The executive director shall attend all meetings of the agency. In the case of an absence or vacancy in the office of the executive director or in the case of disability, the commissioner may appoint an acting executive director to serve as the executive director until the commissioner appoints another executive director. 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.

(i) The commissioner shall appoint a secretary. The secretary shall keep a record of the proceedings of the agency and shall be the custodian and keeper of the records of all books, documents and papers filed by the agency and of its minutes book. The secretary shall cause copies to be made of all minutes and other records and documents of the agency and shall certify that such copies are true copies and all persons dealing with the agency may rely upon such certification.

(j) The chief financial and accounting officer of the agency shall be in charge of its funds, books of account and accounting records. No funds shall be transferred by the agency without the approval of the commissioner and the signatures of the chief financial and accounting officer and the secretary of the agency.

(k) Chapters 268A and 268B shall apply to the commissioner and to employees of the agency; provided, however, that the commissioner 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 agency including, but not limited to: (i) prohibiting the receipt of gifts by the commissioner and employees from any data aggregator, service provider, close associate, affiliate or other person or entity subject to the jurisdiction of the agency; (ii) prohibiting the participation by the commissioner 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 the commissioner in an agency decision due to a potential conflict of interest.

(l) The Massachusetts Data Accountability and Transparency Agency shall be a commission for the purposes of section 3 of chapter 12.

(m) The agency 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 department to manage fiscal operations in the state accounting system and meet statewide and other governmental accounting and audit standards. The agency shall properly classify the agency's operating and capital expenditures, and shall not include any salaries of employees in the agency's capital expenditures. Unless otherwise exempted by law or the applicable central service agency, the agency 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 agency 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 agency shall be subject to section 5D and subsection (f) of section 6B of said chapter 29.

(n) The governor, attorney general, and treasurer and receiver-general shall each appoint one governor respectfully to the board of governors, who shall oversee and manage the funds of the Data Relief Fund; provided, that the three governors shall serve a term of five years and whose replacement shall be appointed in a like manner. The governors shall have a background with similar experience as the commissioner or in finance.

(o) The board of governors shall have the power to create rules, procedures, and management of all funds established in section 7(c) of this chapter.

Section 3. Agency's Purpose, Objectives, and Functions.

(a) The Agency shall seek to protect individuals' privacy and enforce this chapter's limitations on the collection, use, and sharing of personal data and other federal and state privacy law, and is authorized to exercise its authorities under this chapter for such purposes.

(b) The agency is authorized to exercise its authorities under this chapter for the following purposes: (i) protect individuals from violation of this chapter or other federal or state privacy laws or unfair, deceptive, abusive, or discriminatory data practices. (ii) ensure that federal and state privacy law is enforced consistently and in order to protect individuals and ensure fair competition; and (iii) the agency shall work with other agencies to execute their authority under this chapter.

(c) The agency shall function to: (i) provide leadership and coordination to efforts of all state departments and agencies to enforce all laws, executive orders, relations and policy which involve privacy of data protection; (ii) maximize effort, promote efficiency, and eliminate conflict, competition, duplication, and inconsistency among the operations, functions, and jurisdictions of federal and state departments and agencies responsible for privacy or data protection, data protection rights and standards, and fair information practices and principals; (iii) provide active leadership, guidance, education and appropriate assistance to private sector businesses, and organizations, groups, institutions, and individuals regarding privacy, data protection rights and standards, and fair information practices and principals; (iv) require and oversee ex-ante impact assessments and ex-post outcomes audits of high-risk data practices by data aggregators or covered entities to advance fair and just data practices; (v) examining the social, ethical, economic, and civil rights impacts of high-risk data practices and propose remedies; (vi) ensure that data privacy practices are fair, just, and nondiscriminatory, and comply with fair information practices; (vii) collect, research, and respond to complaints; (viii) develop

model privacy, data protection, and fair information practices, standards, guidelines, policies, and routine uses for use by the private sector; (ix) issue rules, orders, and guidance implementing this act; and (x) enforce other privacy statutes and rules as authorized by federal and state law.

(d) The agency and its employees are authorized to exercise its authorities under this chapter to administer, enforce, and otherwise implement the provisions of this chapter.

(e) The agency may require reports and conduct examinations on a periodic basis of data aggregators, who have annual gross revenues that exceed $25,000,000 or who annually collects, uses, or shares, alone or in combination, the personal data of 50,000 or more individuals, households, or devices, for purposes of: (i) assessing compliance with requirements of this chapter or other federal and state laws; (ii) obtaining information of activities subject to such laws and the associated compliance systems or procedures for such entities; (iii) detecting and assessing associated risks to individuals and groups; and (iv) requiring and overseeing ex-ante impact assessments and ex-post outcome audits of automated decision systems to advance fair and just data practices.

(f)(i)The agency may take any action authorized under this chapter to prevent a data aggregator or service provider from committing or engaging in any unfair, deceptive, or abusive acts or practice in connection with the collection, use, or sharing of personal data. (ii) The agency may prescribe regulations applicable to a data aggregator identifying unlawful, unfair, deceptive, or abusive acts or practices in connection with the collection, use, or sharing of personal data, which may include requirements for the purpose of preventing such acts or practices. Rules under this subsection shall not limit, or be interpreted to limit, the scope of unlawful, deceptive, or abusive acts or practices in connection with the collection, use, or sharing

of personal data. (iii) The agency may declare an act or practice in connection with the collection, use, or sharing of personal data to be unlawful on the ground that such act or practice is unfair if the agency has a reasonable basis to conclude that: (A) the act or practice causes or is likely to cause privacy harm or other substantial injury to individuals which is not reasonably avoidable by individuals; and (B) such privacy harm or substantial injury is not outweighed by countervailing benefits to individuals or competition. (iv) The agency may consider established public policies as evidence to be considered with all other evidence but public policy considerations may not serve as a primary basis of such determination. (v) The agency may declare an act or practice abusive in connection with the collection, use, or sharing of personal data if the act or practice: (A) materially interferes with the ability of an individual to understand a term of condition of a good or service; or (B) takes unreasonable advantage of a lack of understanding on the part of the individual of the material risks, costs, or conditions of the product or service; the inability of the individual to protect their interests in selecting or using a product or service; or the reasonable reliance by the individual on a data aggregator or service provider to act in the interests of the individual; and (vi) The agency may limit or require the divestment of any lines of business in which any data aggregator participates based on antitrust or competition concerns and have the authority to review and approve any merger between a data aggregator and any other company whose business is conducted in Massachusetts.

(g) It shall be unlawful for; (i) any data aggregator or service provider to commit any act or omission in violation of this chapter or other data privacy law; or to engage in any unfair, deceptive, or abusive act or practice relating to personal data; (ii) any data aggregator or service provider to fail or refuse, as required by this chapter or other privacy law, or any rule or order issued by the agency thereunder to: (A) permit access to or copying of records; (B) establish or

maintain records; or (C) to make reports or provide information to the agency; or (iii) any person to knowingly or recklessly provide substantial assistance to a data aggregator or service provider in violation of this section or other data privacy laws, or any rule issued thereunder, and notwithstanding any provision of this act, the provider of such substantial assistance shall be deemed to be in violation of this chapter or other law to the same extent as the person whom substantial assistance is provided.

Section 4. Agency Enforcement.

(a) The agency or, where appropriate, an agency investigator, may engage in independent or joint investigations and requests for information, as authorized under this chapter.

(b) The authority under subsection (a), includes matters relating to protection of individuals' civil rights under this chapter and joint investigations with, and requests for information from, the Consumer Financial Protection Bureau, the Federal Trade Commission, the Department of Health and Human Services, the Department of Education, the office of the United States Attorney General, the office of the Massachusetts Attorney General, the Massachusetts executive office of health and human services, the Massachusetts department of public health, and all other federal and state agencies with oversight of data privacy to promote consistent regulatory treatment across all governmental bodies.

(c) The agency, commissioner, employee, or agency investigator may issue subpoenas for the attendance and testimony of witnesses and the production of relevant papers, books, documents, or other material in connection with hearings or investigations under this chapter.

(d) In the case of contumacy or refusal to obey a subpoena issued by the agency, pursuant to this section, and served upon any person, the Superior Court of Massachusetts, upon

application by the agency, commissioner, employee, or agency investigator and after notice to such person, may issue an order requiring such person to appear and give testimony or to appear and produce documents or other material. Any failure to obey an order of the court under this section may be punished by the court as contempt thereof.

(e) The agency may conduct hearings, adjudicatory proceedings, write advisory rulings, and promulgate regulations in accordance with chapter 30A.

(f) The Massachusetts Superior Court shall have jurisdiction over all appeals of agency adjudicatory rulings and decisions.

(g) Whenever the agency has reason to believe that any person may be in possession, custody, or control of any private data, documentary material or tangible things, or may have any information, relevant to a violation of this chapter, the agency may issue in writing, and cause to be served upon such person, a civil investigative demand, consistent with Chapter 93A of the Massachusetts General Laws, and in coordination with the Massachusetts attorney general's office.

(h) Whenever any person fails to comply with any civil investigative demand duly served upon such person, under this section, or whenever satisfactory copying or reproduction of material requested pursuant to the demand cannot be accomplished and such person refuses to surrender such material, the agency, in coordination with the Massachusetts attorney general's office, through such offers or attorneys as it may designate, may file, in Superior Court for an order of the court to enforce this chapter.

(i) If, in the opinion of the agency, any data aggregator is engaging or has engaged in an activity that violates a law, rule, or any condition imposed in writing on the person by the

agency, the Agency may issue and serve upon the data aggregator or service provider a notice of charges in respect thereof. The notice shall contain a statement of facts constituting the alleged violation or violations, and shall fix a time and place at which a hearing will be held to determine whether an order to cease and desist should issue against the data aggregator or service provider. Such hearing shall be held not earlier than 30 days nor later than 60 days after the date of service of such notice, unless an earlier or later date is set by the agency, at the request of the party served.

(j) If the agency finds that any violation specified in the notice of charges has been established, the Agency may issue and serve upon the data aggregator or service provider an order to cease- and-desist from the violation or practice. Such order may, by provisions which may be mandatory or otherwise, require the data aggregator or service provider to cease and desist from the subject activity, and to take affirmative action to correct the conditions resulting from any such violation.

(k) The agency may at any time, upon such notice and in such manner as the agency shall determine proper, modify, terminate, or set aside any such order. Upon filing of the record as provided, the agency may modify, terminate, or set aside any such order with permission of the court.

(l) Data aggregators, service providers, and persons may appeal a cease-and-desist order to the Superior Court within 10 days of being served such order.

(m) The agency may issue a temporary order requiring: (i) the cessation of any activity or practice which gave rise, whether in whole or in part, to the incomplete or inaccurate state of the

books or records; or (ii) affirmative action to restore such books or records to a complete and accurate state, until the completion of the proceedings.

(n) The agency in its discretion may apply to the Superior Court for the enforcement of any effective and outstanding notice or order issued under this section, and such court shall have jurisdiction and power to order and require compliance with this chapter.

(o) If any person violates this act, the agency may commence a civil action against such person to impose a civil penalty or to seek all appropriate legal and equitable relief including a permanent or temporary injuction as permitted by law. The agency may act in its own name and through its own attorneys in enforcing any provision of this chapter.

(p) The agency may compromise or settle any action if such compromise is approved by the Superior Court.

(q) The agency shall notify the attorney general concerning any action, suit, or proceeding to which the agency is a party and shall consult regarding the coordination of investigations and proceedings, including by negotiating an agreement for coordination on investigations and proceedings.

(r) In an action or adjudication proceeding brought under this chapter, the court or the agency shall have jurisdiction to grant any appropriate legal or equitable relief with respect to a violation of this chapter or regulations promulgated through this chapter. Relief under this section shall include, but not be limited to: (i) rescission or reformation of contracts; (ii) refund of moneys or return of real property; (iii) restitution; (iv) disgorgement or compensation for unjust enrichment; (v) payment of damages or other monetary relief; (vi) public notification

regarding the violation, including the costs of notification; (vii) limits on the activities or functions of the person; and (viii) civil money penalties.

(s) The agency, attorney general's office and any other agency or division of the commonwealth may recover the costs in connection with prosecuting such action if the agency is the prevailing party in the action.

(t) Any person that violates, through any act or omission, any provision of this chapter shall forfeit and pay a civil penalty: (i) for any violation of a law, rule, or final order or condition imposed in writing by the agency, a civil penalty may not exceed $5,000 for each day during which such violation or failure to pay continues; (ii) not withstanding clause (i), for any person that recklessly engages in a violation of this chapter, a civil penalty may not exceed $25,000 for each day during which such violation continues; and (iii) any person that re-identifies, or attempts to re-identify, anonymized data shall be assessed a fine of $25,000 per attempt, not to exceed $1,000,000 per day.

(u) In determining the amount of any penalty assessed under this section, the agency or court shall take into account the appropriateness of the penalty with respect to: (i) the size of financial resources and good faith of the person charged; (ii) the gravity of the violation or failure to pay; (iii) the severity of the risks of harms to the individual; (iv) the history of previous violations; and (v) such other matters as justice may require.

(v) The agency may compromise, modify, or remit any penalty which may be assessed or had already been assessed under this chapter.

(w) If the agency obtains evidence that any person has engaged in conduct that may constitute a violation of this chapter or other privacy laws, the agency shall transmit such

evidence to the Massachusetts attorney general who may institute criminal proceedings under the appropriate law.

Section 5. Agency Offices and Departments.

(a) The commissioner shall establish offices, divisions or departments within the agency that shall include, but not be limited to an office of: (i) Civil Rights; (ii) Complaints; (iii) Enforcement; and (iv) Data Privacy Research.

(b) The office of Civil Rights shall: (i) provide oversight and enforcement of this chapter to ensure that the collection, use, and sharing of personal data is fair, equitable, and nondiscriminatory; (ii) coordinate the agency's civil rights efforts with other federal agencies, state agencies, regulators and constitutional officers to promote consistent, efficient, and effective enforcement of federal and state civil rights laws; (iii) work with civil rights and data privacy organizations and industry to promote compliance with civil rights compliance under this act; and (iv) file annual reports with the office of the governor, attorney general, treasurer and receiver-general and publish these reports online on the agency's website.

(c) The complaints division shall manage all consumer complaints from individuals who allege privacy harm by data aggregators. The commissioner shall establish within the complaints division a single toll-free telephone number, a publicly available website, and a publicly available database, to facilitate the centralized collection of, monitoring of, and response to complaints regarding the collection, use, and sharing of personal data.

(d) The enforcement division shall: (i) manage all investigations; (ii) work with legal counsel on all adjudicatory proceedings, subpoenas, notice of charges, cease-and-desist orders, and appeals.

(e) The data privacy research division shall study, analyze and report on developments regarding data privacy, data collection and use of personal data, study of automated decision systems and all other pertinent topics relative to the improvement of individual's data privacy in the state.

Section 6. Website and Database.

(a) The agency shall create and maintain a publicly available website and database through which data aggregators shall report the types of personal data that those data aggregators collect, use, or share and an individual may exercise rights, established under this chapter, with respect to the personal data of the individual.

(b) The agency shall maintain a publicly accessible list of data aggregators that collect, use, or share personal data of more than 10,000 persons or households, and the permissible purposes for which the data aggregators purport to collect personal data.

(c) The agency shall order that the landing page of the agency's main website contain a clear and conspicuous hyperlink to the complaint database and shall: (i) order that such database is user-friendly and in plain writing; (ii) ensure that all complaints are available to the public and shall place a clear and conspicuous hyperlink on the landing page of the main website of the agency that contains a searchable and sortable list of complaints; provided, that the complaints available to the public shall have all personal data removed; (iii) ensure that the website explains how to file a complaint with the agency, where to find reports of the agency, what offices are within the agency, the offices or division's responsibilities, what research has been conducted by the agency, the results of the research and why the research was conducted; and (iv) translate all

consumer guidance documents on the agency's website into the five most common languages spoken in Massachusetts.

Section 7. Funding Penalties and Fines.

(a) There shall be on the books of the commonwealth a fund titled the Data Accountability Fund. The commissioner may collect an assessment, fee, or other charge from a data aggregator that has annual gross revenues that exceed $25,000,000, or annually collects, uses, or shares, alone or in combination, the personal data of 50,000 or more individuals, households or devices; and provided further, that the commissioner shall determine the manner of payment, and disbursement expenses allowed.

(b) 50 per cent of the amounts transferred to the agency under paragraph (a) shall be deposited into the Data Accountability Fund which may be used by the commissioner in accordance with this act.

(c) There shall be a separate fund on the books of the commonwealth that shall be titled the Data Relief Fund that shall be established and maintained to assist relief for individuals harmed by data aggregators.

(d) 50 per cent of the amounts transferred to the agency under paragraph (a) shall be deposited into the Data Relief Fund.

(e) By a majority vote, the board of governors shall determine the investment in the Data Relief Fund money and disbursement to individuals who were victims of privacy harm.

(f) No amount transferred to the agency under paragraph (a) shall be deposited into the general fund.

Section 8. Annual Reports.

(a) The agency shall file annual reports with the office of the governor, attorney general, treasurer and receiver-general and publish these annual reports online, on the agency's website. (b) The annual report shall include: (i) a discussion of the significant problems faced by individuals in exercising their rights under this act; (ii) a justification of the budget request of the previous year; (iii) a list of significant rules and orders adopted by the agency, as well as other significant initiatives conducted by the agency, during the preceding year and plan of the agency for rules, orders, or other initiatives to be undertaken during the upcoming period; (iv) analysis of complaints about practices relating to the collection, use, or sharing of protected data that the agency has received and collected in its central database on complaints during the preceding year; (v) a list, with a brief statement of issues of the public supervisory and enforcement actions to which the agency was a party during the preceding year; (vi) the actions taken regarding rules, orders, and supervisory actions with respect to data aggregators; (vii) an assessment of significant actions by the Massachusetts attorney general, state attorneys general or other state regulators relating to this chapter; (viii) an analysis of the efforts of the agency to fulfill the civil rights in data mission of the agency; and (ix) and analysis of the efforts of the agency to increase workforce and contracting diversity.

Section 9. Requirements for Data Aggregators.

(a) Data aggregators shall not collect, use, or share, or cause to be collected, used, or shared any personal data unless the data aggregator can demonstrate that such personal data is strictly necessary to carry out a permissible purposed under subsection (b).

(b) A data aggregator may not collect, use, or share personal data unless strictly necessary to carry out one or more of the following permissible purposes: (i) to provide a good, service, or specific feature requested by an individual in an intentional interaction; (ii) to engage in journalism, provided that the data aggregator has reasonable safeguards and processes that prevent the collection, use, or sharing of personal data; (iii) to conduct public or peer-reviewed scientific, historical, or statistical research in the public interest, but only to the extent such research is not possible using anonymized data; (iv) to employ an individual, including for administration of wages and benefits, except that a data aggregator may not invasively collect, use, or share the employee's personal data in carrying out this paragraph; (v) to comply with law; (vi) consistent with due process, direct compliance with a civil, criminal, or regulatory inquiry, investigation, subpoena or summons; (vii) to bring or defend legal claims, provided that the parties or potential parties take all necessary measures, including, as applicable, obtaining a protective order, to protect against unnecessary public disclosure of personal data; (viii) to detect or respond to security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity; (ix) free expression by individuals on a social network or media platform; (x) in exigent circumstances, if first responders or medical personnel, in good faith, believe danger of death or serious physical injury to an individual, or danger of serious and unlawful injury to property, requires collection, use, or sharing of personal data relating to the exigent circumstances; (xi) the development and delivery of advertisements: (A) based on the content of the website, online service, or application to which the individual or device is connected; and (B) excludes adverting based on the use of any personal data collected or stored from previous interactions with the individual or device, a profile of the individual or device, or the previous online or offline behavior of the individual or device; or (xii) to offer

discounted or free goods or services to an individual if: (A) the offering is in connection with the voluntary participation by the individual in a program that rewards patronage; and (B) personal data is only collected to track purchases for loyalty rewards under the program described in (A).

(c) Except where strictly necessary to carry out a permissible purpose, a data aggregator shall not: (i) share personal data with affiliated entities, service providers, or third parties; (ii) use personal data for any purpose other than to carry out a permissible purpose; (iii) retain personal data for longer than strictly necessary to carry out a permissible purpose; or (iv) derive or infer data from any element or set of personal data; and (v) collecting, using, or sharing personal data to generate advertising revenue to support or carry out a permissible purpose is not a permissible purpose.

(d)(i) It is unlawful for a person to engage or cause to be engaged in the following practices: (A) charge an extra fee or raise the price for a good, service, or feature when a person exercises the rights of the person under this chapter; (B) terminate, refuse to provide, degrade goods or services to, or otherwise retaliate against, a person that exercises the rights of the person under this act; (C) re-identify, or attempt to re-identify, an individual, household, or device from anonymized data, unless conducting authorized testing to prove personal data has been anonymized; and (D) commingle personal data from multiple applications, services, affiliates, or independent business lines. (ii) It is unlawful for any data aggregator to: (A) use facial recognition technology; or (B) collect, use or share any personal data obtained from facial recognition technology. (iii) A person is prohibited from engaging in the unlawful data practices in paragraph (d)(i) regardless of whether such person has a permissible purpose for collecting, using, or sharing personal data. (iv) In addition to relief available under section 14, a data aggregator shall be subject to treble damages for a violation of this section.

(e) It shall be unlawful for a data aggregator to collect, use, or share personal data for advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for housing, employment, credit, or insurance in a manner that discriminates against or otherwise makes the opportunity unavailable or offered on different terms on the basis of a protected class or otherwise materially contributes to unlawful discrimination.

(f) It shall be unlawful for a data aggregator to collect, use, or share personal data in a manner that segregates, discriminates in, or otherwise makes unavailable the good, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of a protected class.

(g) It shall be unlawful for a data aggregator to: (i) withhold, deny, deprive, or attempt to withhold, deny, or deprive any individual of any right or privilege secured by this chapter; (ii) intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any individual with the purpose of interfering with any right or privilege secured by this section; or (iii) punish or attempt to punish any individual for exercising or attempting to exercise any right or privilege secured by this section.

(h) It shall be unlawful for a person to use personal data in a manner that deprives, defrauds, or attempts to deprive or defraud an individual of the free and fair exercise of the right to vote in a Federal, State, or local election. Intentionally depriving defrauding or attempting to deprive or defraud includes: (i) deception as to the times, places, or methods of voting; eligibility to vote; counting of ballots; adjudications of elections; explicit endorsements by any person of a candidate; or other material information pertaining to the procedures or requirements for voting

or registering to vote in a Federal, State, or local election; or (ii) using deception, threats, intimidation, or coercion to prevent, interfere with, retaliate against, deter, or attempt to prevent, interfere with, retaliate against, or deter: (A) voting or registering to vote in a Federal, State, or local election; or (B) giving support or advocacy in a legal manner toward a candidate in a Federal, State, or local election.

(i) It shall be unlawful for any data aggregator to discriminate against an individual because the individual exercised any of their rights under this chapter, or did not agree to the use of their personal data for a separate product or service, including by: (i) denying goods or services; (ii) charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; (iii) providing a different level or quality of goods or services; and (iv) suggesting that an individual will receive a different price or rate for goods or services or a different level or quality of goods or services.

(j) If the use of personal data causes a disparate impact on the basis of a protected class under this section, the data aggregator has the burden of demonstrating that such use of personal data: (i) is not intentionally discriminatory; (ii) is strictly necessary to achieve one or more substantial, legitimate, nondiscriminatory interests; and (iii) there is no reasonable alternative policy or practice that could serve the interest described in paragraph (ii) with a less discriminatory effect.

Section 10. Algorithmic Accountability.

(a) If a data aggregator utilizes automated decision systems, the data aggregator shall perform: (i) continuous and automated testing for bias on the basis of a protected class; and (ii)

continuous and automated testing for disparate impact on the basis of a protected class as required by the agency.

(b) When evaluating an automated decision system against other less discriminatory alternative, similar methodology shall be used to create the alternatives.

(c) For any automated decision system, a data aggregator shall provide the agency: (i) an automated decision system risk assessment, within 90 days for any automated decision system currently in use; prior to the deployment of any new automated decision system; or as determined by the commissioner; and (ii) an automated decision system impact evaluation on a periodic basis as determined by the commissioner, but no less than annually.

(d) The agency shall make automated decision system impact evaluations publicly available and shall be published on the agency's website.

Section 11. Individual Rights.

(a) Upon receipt of a verifiable request, a data aggregator shall provide the: (i) specific pieces of personal data collected, used, or shared about the individual; (ii) permissible purposes for such collection, use, or sharing of an individual's personal data at the time of collection, use, or sharing; (iii) service providers or third parties with which it has shared the personal data; and (iv) individual's personal data in an electronic, portable, machine-readable, and readily useable format or formats to the individual, or to another person of the individual's choice.

(b) A data aggregator shall disclose the following information, including in its online privacy policy: (i) a description of an individual's rights under this chapter and designated methods for summitting verifiable requests; (ii) a description of the personal data that the data

aggregator collects, uses, or shares; (iii) the specific sources from which personal data is collected; (iv) a description of the sources from which personal data is collected; (v) the permissible purposes for which personal data is collected, used, or shared; (vi) the affiliates, service providers, or third parties with which the data aggregators shares personal data, and the permissible purpose for such sharing; (vii) a description of the length of time for which personal data is retained; and (viii) if personal data is collected and retailed as anonymized data, a description of the techniques and methods used to create the anonymized data.

(c) A data aggregator shall maintain reasonable policies and procedures to ensure that any personal data that it collects, uses or shares is accurate. An individual has the right to require that a data aggregator that retains the individual's personal data correct any inaccurate or incomplete personal data. Upon receipt of a verifiable request, a data aggregator shall correct and inaccurate or incomplete personal data, as directed by that individual, and direct any service provider to correct the individual's personal data in its records.

(d) An individual has the right to request that a data aggregator delete any personal data that the data aggregator has collected about the individual. Unless strictly necessary to carry out a permissible purpose under Section 9, upon receipt of a verifiable request, a data aggregator shall delete the personal data of such individual, and direct any service providers to delete such individual's personal data from its records.

(e) An individual has the right to object to the claimed permissible purpose for any personal data that a data aggregator has collected, used, or shared of such individual. Upon receipt of an individual's verifiable request that objects to the data aggregator's claimed permissible purpose for collecting, using, or sharing such individual's personal data, a data

aggregator shall produce evidence supporting the data aggregator's claim that the collection, use, or sharing of such individual's personal data: (i) was strictly necessary to carry out a permissible purpose; (ii) was not used or shared for any other purpose; and (iii) has not been retained for any time longer than strictly necessary to carry out a permissible purpose.

(f) For any material decision by a data aggregator based on automated processing of personal data of an individual, a data aggregator shall: (i) inform the individual of the specific personal data that was used for such a decision; (ii) make available an easily available mechanism by which the individual may request human review of such decisions; and (iii) upon receipt of a verifiable request for a human review of material decision, conduct such a review within 15 days of the date of the request.

Section 12. Duty of care.

(a) A data aggregator shall implement and maintain reasonable security procedures and practices, including administrative, physical, and technical safeguards, appropriate to the nature of the personal data and the purposes for which the personal data will be collected, used, or shared, to ensure that personal data: (i) is only collected, used, or shared where strictly necessary to carry out a permissible purpose under Section 9; (ii) is not retained for any time longer than strictly necessary to carry out a permissible purpose under Section 9; and (iii) is protected from unauthorized collection, use, sharing, or disclosure.

(b) A data aggregator: (i) shall ensure that the service providers of the data aggregator comply with the requirements of this chapter; and (ii) is liable for any violation of this chapter by its service providers.

Section 13. Duties of Data Aggregator Upon Receipt of Verifiable Request.

(a) A data aggregator is prohibited from charging any fee to carry out a verifiable request under this chapter.

(b) A data aggregator shall carry out a verifiable request within 30 days of receiving the verifiable request.

(c) The requirements of this chapter shall not apply if the data aggregator receiving a verifiable request determines that the verifiable request is frivolous or irrelevant, including by reason of: (i) the failure of the individual to provide sufficient information to carry out the verifiable request; or (ii) the verifiable request is substantially the same as a verifiable request previously submitted by the individual, with respect to which the person has already performed the data aggregator's duties under this chapter.

Section 14. Private Right of Action.

(a) Any person may commence a civil action: (i) against any person, including the commonwealth of Massachusetts or any other governmental instrumentality or agency to the extent permitted by the Eleventh Amendment to the Constitution of the United States, that is alleged to have violated this chapter; or (ii) against the agency if the agency is alleged to have: (A) adopted a rule in violations of any provision of chapter 30A of the general laws; or any provision of this chapter; or (B) failed to promulgate a rule required under this chapter, in order to compel the issuance of such rule.

(b) The Superior Court of Massachusetts shall have jurisdiction over all civil actions in subsection (a).

(c) In a civil action brought under (a)(i), in which the plaintiff prevails, the court may award: (i) an amount not less than $100, and not greater than $1,000, per violation per day or actual damages, whichever is greater; (ii) punitive damages; (3) reasonable attorney's fees and litigation costs; and (4) any other relief, including a temporary or permanent injunction, equitable, or declaratory relief, that the court determines appropriate.

(d) A violation of this chapter or a regulation promulgated under this chapter is presumed to cause privacy harm and constitutes a concrete and particularized injury in fact to that individual.

Section 15. Corporate Accountability.

(a) Each data aggregator shall establish comprehensive privacy and data security policies, procedures, and practices to ensure compliance with this act.

(b) Each data aggregator shall submit to the agency an annual report: (i) describing its collection, use, or sharing of personal data, and the permissible purpose for such collection, use, or sharing of personal data; (ii) identifying each service provider with which the data aggregator shares personal data, the permissible purposes for sharing personal data with each such service provider, and a description of the oversight and supervision conducted by the data aggregator to ensure that each such service provider complies with the requirements of this chapter; (iii) internal controls that the data aggregator has put in place to ensure compliance with the requirements of this chapter; and (iv) a description of the testing, and results of such testing, to ensure compliance with the requirements of this act.

(c) The chief executive officer or, if the data aggregator does not have a chief executive officer, the highest ranking officer of the data aggregator, shall annually certify to the agency

that it has complied with this chapter, including: (i) conducted oversight sufficient to demonstrate all service providers are complying with this chapter; (ii) maintains adequate internal control sufficient to demonstrate compliance with this chapter; (iii) conducted testing sufficient to demonstrate compliance with this act; and (iv) maintains reporting structures to ensure that the chief executive officer, or if a chief executive officer does not exist, the highest ranking officer that is involved in, and responsible for, decisions to ensure compliance with this chapter.

Section 16. Criminal and Civil Penalties for CEO and Board of Directors.

(a) Criminal Penalty. Whoever knowingly and intentionally violates, or knowingly and intentionally attempts to violate, sections 9, 10, or 15, shall be fined $250,000, or imprisoned for not more than five years, or both.

(b) Whoever violates, or attempts to violate, sections 9, 10, or 15 while violating another law or as part of a pattern of any illegal activity involving more than $100,000 in a 12-month period shall be fined twice the amount provided in subsection (a) for individuals and for $1,000,000 for organizations, or imprisoned for not more than 10 years, or both.

(c) Whoever violates this section shall be liable to the state of Massachusetts for a civil fine of not more than $10,000,000.

Section 17. Whistle Blower Protections.

(a) A data aggregator may not, directly or indirectly, discharge, threaten, harass, suspend, demote, terminate, or in any other manner discriminate against a covered individual because (i) the covered individual, or anyone perceived as assisting the covered individual, takes, or the data

aggregator suspects that the covered individual has taken or will take, a lawful action in providing to the government or the attorney general of Massachusetts information relating to any act or omission that the covered individual reasonably believes to be a violation of this chapter or any regulation promulgated under this chapter; (ii) the covered individual provides information that the covered individual reasonably believes evidences such a violation to: (A) a person with a supervisory authority over the covered individual at the covered entity; or (B) another individual working for the covered entity who the covered entity reasonably believes has the authority to investigate, discover, or terminate the violation or to take any other action to address the violation; (iii) the covered individual testifies, or the covered entity expects that the covered individual will testify, in an investigation or judicial or administrative proceeding concerning such a violation; (iv) the covered individual assists or participates in such an investigation or judicial or administrative proceeding; or (v) take any other action to assist in carrying out the purposes of this chapter.

(b) An individual who alleges discharge or other discrimination in violation of subsection (a) may bring an action governed by the rules, procedures, statute of limitations, and legal burdens of proof in section 185 of chapter 149 of the Massachusetts General Laws. If the individual has not received a decision within 180 days and there is no showing of bad faith of the claimant, the individual may bring an action for a jury trial in Massachusetts Superior Court, for the following relief: (i) temporary relief while case is pending; (ii) reinstatement of senority, but for the discharge or discrimination; (iii) three times the amount of back pay otherwise owed to the individual, with interest; and (iv) consequential and compensatory damages, and compensation for litigation costs, expert witness fees, and reasonable attorneys' fees.

Section 18. Waiver of Rights and Remedies.

No provisioner of this chapter may be waived and any agreement to waive compliance with or modify any provision of this chapter shall be void as contrary to public policy.

Section 19 Severability.

If any provision of this chapter or the application of such provision is held to be unconstitutional, the remainder of this chapter, and the application of the provisions of such to any person or circumstances, shall not be affected thereby.

SECTION 2. Section 8 of Chapter 223 is hereby amended by striking out the paragraph after the words “the state racing commission,” and inserting the following:-

the Massachusetts Data Accountability and Transparency Agency, the parole board or a board of appeals designated or appointed under section thirty of chapter forty, as to matters within their authority; and such witnesses shall be summoned in the same manner, be paid the same fees and be subject to the same penalties for default, as witnesses in civil cases before the courts. The presiding officer of such council, or of either branch thereof, or a member of any such committee, board or commission, or any such commissioner, may administer oaths to witnesses who appear before such council, branch thereof, committee, board, commission or commissioner, or agency respectively.

SECTION 3. Section 2 of chapter 32A of the General Laws, as so appearing, is hereby amended by inserting after the words “Massachusetts cannabis control commission”, in lines 13 and 14, the following words:- Massachusetts Data Accountability and Transparency Agency,

SECTION 4. Section 2 of Chapter 93A of the General Laws, is hereby amended by adding the following subsection:-

(d) The attorney general shall coordinate with the Massachusetts Data Accountability and Transparency Agency regarding violations of chapter 93L of the General Laws.

SECTION 5. Chapter 12 of the General Laws, is hereby amended by adding the following section:-

Section 35.

(a) The attorney general shall have the power to enforce all of Chapter 93L in coordination with the Massachusetts Data Accountability and Transparency Agency.

(b) The attorney general shall promulgate regulations to enforce this section and Chapter 93L.

(c) The attorney general shall coordinate with the Massachusetts Data Accountability and Transparency Agency and negotiate an agreement regarding investigations and proceedings.

(d) The attorney general shall ensure uniformity in data privacy laws across the state.