

SENATE No. 120

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 relative to consumer data privacy.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	
<i>Cynthia Stone Creem</i>	<i>First Middlesex and Norfolk</i>	
<i>Tommy Vitolo</i>	<i>15th Norfolk</i>	<i>1/30/2019</i>
<i>Michael O. Moore</i>	<i>Second Worcester</i>	<i>2/1/2019</i>
<i>James B. Eldridge</i>	<i>Middlesex and Worcester</i>	<i>2/1/2019</i>

SENATE No. 120

By Ms. Creem, a petition (accompanied by bill, Senate, No. 120) of Cynthia Stone Creem, Tommy Vitolo, Michael O. Moore and James B. Eldridge for legislation relative to consumer data privacy. Consumer Protection and Professional Licensure.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-First General Court
(2019-2020)

An Act relative to consumer 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:

1 SECTION 1. The General Laws are hereby amended by inserting after chapter 93K the
2 following chapter:-

3 CHAPTER 93L.

4 Consumer Data Privacy.

5 Section 1. Definitions.

6 As used in this chapter, the following words shall, unless the context clearly requires
7 otherwise, have the following meanings:

8 (a) “Aggregate consumer information” means information that relates to a group or
9 category of consumers, from which individual consumer identities have been removed, that is
10 not linked or reasonably linkable to any consumer, including via a device. “Aggregate consumer

information” does not mean one or more individual consumer records that have been de-identified.

(b) “Biometric information” means an individual’s physiological, biological or behavioral characteristics, including an individual’s DNA, that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) “Business” means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is:

(A) organized or operated for the profit or financial benefit of its shareholders or other owners;

(B) that collects Massachusetts consumers’ personal information; and

(C) Satisfies one or more of the following thresholds:

(i) Has annual gross revenues in excess of \$10,000,000, as adjusted pursuant to paragraph (5) of subdivision (a) of section 11; or

(ii) Derives 50 percent or more of its annual revenues from third party disclosure of consumers’ personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. “Control” or “controlled” means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. “Common branding” means a shared name, servicemark, or trademark.

(d) “Business purpose” means the reason for the use of personal information by a business or a service provider.

(e) “Collects,” “collected,” or “collection” means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer’s behavior.

(f) “Consumer” means a natural person who resides in the Commonwealth.

(g) “Deidentified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;

(2) Has implemented business processes that specifically prohibit reidentification of the information;

(3) Has implemented business processes to prevent inadvertent release of deidentified information; and

(4) Makes no attempt to reidentify the information.

(h) “Designated methods for submitting requests” means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this chapter, and any new, consumer-friendly means of contacting a business, as approved by the attorney general pursuant to paragraph (4) of subdivision (a) of section 11.

(i) “Device” means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.

(j) “Homepage” means the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application’s platform page or download page, a link within the application, such as from the application configuration, “About,” “Information,” or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of section 2, including, but not limited to, before downloading the application.

(k) “Infer” or “inference” means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(l) “Person” means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(m) (1) “Personal information” means any information relating to an identified or identifiable consumer. “Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or the consumer’s device.

(2) “Personal information” does not include publicly available information. For these purposes, “publicly available” means information that is lawfully made available from federal, state, or local government records. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge.

(3) “Personal information” does not include consumer information that is deidentified or aggregate consumer information.

(n) “Probabilistic identifier” means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(o) “Processing” means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(p) “Pseudonymize” or “Pseudonymization” means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(q) “Research” means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer’s interactions with a business’s service or device for other purposes shall be:

(1) Used solely for research purposes which are compatible with the context in which the personal information was collected;

(2) Not be used for any commercial purpose;

(3) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer;

(4) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;

(5) Subject to business processes that specifically prohibit reidentification of the information;

(6) Made subject to business processes to prevent inadvertent release of deidentified information;

(7) Protected from any reidentification attempts; and

(8) Subjected by the business conducting the research to additional security controls limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

(r) “Service” or “services” means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(s) “Service provider” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this chapter.

(t) “Third party” means a person who is not the business that collects personal information from consumers under this chapter or a service provider of that business.

(u) “Third party disclosure” means any transfer of a consumer’s personal information by the business to a third party including, but not limited to, selling, renting, releasing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means.

For purposes of this chapter, a business does not engage in third party disclosure when:

(1) The business discloses personal information of a consumer to a service provider who is necessary to the performance of a business purpose which is included in a Section 2 notice.

(2) The business identifies a consumer who has opted out of the sale of the consumer's personal information for the purpose of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(3) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with the notice received by consumers in Section 2. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their rights under this chapter. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the provisions of chapter 93A prohibiting unfair and deceptive practices.

(v) "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer or a device that is linked to a consumer, over time and across different services, including, but not limited to:

(a) a device identifier;

(b) an Internet Protocol address;

(c) cookies, beacons, pixel tags, mobile ad identifiers, or similar technology;

(d) consumer number, unique pseudonym, or user alias; or

(e) telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.

(w) “Verifiable consumer request” means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the attorney general pursuant to section 11 to be the consumer about whom the business has collected personal information.

Section 2. Notice At or Before Collection

(a) A business that collects a consumer’s personal information shall, at or before the point of collection, notify a consumer of:

- (1) The categories of personal information it will collect about that consumer;
- (2) The business purposes for which the categories of personal information shall be used;
- (3) The categories of third parties with whom the business discloses personal information;
- (4) The business purpose for third party disclosure; and
- (5) The consumer’s rights to request:
 - (A) A copy of the consumer’s personal information, pursuant to section (3);
 - (B) The deletion of the consumer’s personal information, pursuant to section (5); and

(c) Opt-out of third party disclosure, pursuant to section (6).

(b) A business shall not collect additional categories of personal information or use personal information collected for additional purposes without first providing the consumer with notice consistent with this section.

Section 3. Verifiable Consumer Requests

(a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer:

(1) The specific pieces of personal information the business has collected about that consumer;

(2) The sources from which the consumer's personal information was collected;

(3) The names of third parties to whom the business disclosed the consumer's personal information; and

(4) The business purpose for third party disclosure.

(b) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(c) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this

information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(d) This section shall not require a business to:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained;

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information; or

(3) Disclose any specific personal information that would adversely affect the legal rights of other consumers.

(e) If verified requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request.

Section 4. Mechanism for Verifiable Consumer Requests.

(a) In order to comply with the sections of this chapter, a business shall, in a form that is reasonably accessible to consumers make available to consumers two or more designated methods for submitting consumer verified requests, including, if the business maintains an

internet web site, a link on the home page of the web site. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.

(b) In order to comply with the sections of this chapter, a business shall, deliver to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer the information required in section 3 in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.

(c) A business is not obligated to provide the information required by section 3 to the same consumer more than twice in a 12-month period.

(d) A business shall include the following information in its online privacy policy or policies if the business has an online privacy policy or policies, or if the business does not maintain those policies, on its Internet Web site, and update that information at least once every 12 months:

- (1) The categories of personal information the business collects about consumers;
- (2) The business purposes for which the categories of personal information are used;
- (3) The categories of third parties with whom the business discloses personal information;
- (4) The business purpose for third party disclosure; and
- (5) The consumer's rights to request:

- 234 (A) A copy of the consumer's personal information, pursuant to section (3);
- 235 (B) The deletion of the consumer's personal information, pursuant to section (5); and
- 236 (c) Opt-out of third party disclosure, pursuant to section (6).

237 (e) A business shall ensure that all individuals responsible for handling consumer

238 inquiries about the business's privacy practices or the business's compliance with this chapter

239 are informed of all requirements in this chapter and how to direct consumers to exercise their

240 rights.

241 (f) A business shall use any personal information collected from the consumer in

242 connection with the business's verification of the consumer's request solely for the purposes of

243 verification.

244 5. Right to Delete.

245 (a) A consumer shall have the right to request that a business delete any personal

246 information about the consumer which the business has collected from the consumer.

247 (b) A business that collects personal information about consumers shall disclose, pursuant

248 to section 2, the consumer's rights to request the deletion of the consumer's personal

249 information.

250 (c) A business that receives a verifiable consumer request from a consumer to delete the

251 consumer's personal information pursuant to subdivision (a) of this section shall delete the

252 consumer's personal information from its records and direct any service providers to delete the

253 consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer;

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity;

(3) Identify or repair errors that impair existing intended functionality;

(4) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law;

(5) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent; or

(6) Comply with a legal obligation.

Section 6. Right to Opt-out of Third Party Disclosure.

(a) A consumer shall have the right, at any time, to demand that a business not disclose the consumer's personal information to third parties. This right may be referred to as the right to opt-out of third part disclosure.

(b) Notwithstanding subdivision (a), a business shall not disclose the personal information of a consumer to a third party if the business has actual knowledge or willfully disregards the fact that the consumer is less than 18 years of age.

(c) A business that has received direction from a consumer not to disclose the consumer's personal information to third parties shall be prohibited from such disclosure unless the consumer later provides express authorization for that disclosure. However, a business shall not request such authorization for at least 12 months.

(d) In order to comply with this section, a business shall provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Share My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the third party disclosure of the consumer's personal information. A business shall not require a consumer to create an account in order to exercise this right.

(e) A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the attorney general.

Section 7. No Penalty for Exercise of Rights.

A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this chapter, including, but not limited to, by:

(a) Denying goods or services to the consumer;

295 (b) Charging different prices or rates for goods or services, including through the use of
296 discounts or other benefits or imposing penalties;

297 (c) Providing a different level or quality of goods or services to the consumer; or

298 (d) Suggesting that the consumer will receive a different price or rate for goods or
299 services or a different level or quality of goods or services.

300 Section 8. Exemptions.

301 (a) The obligations imposed by this chapter shall not restrict any business or third party's
302 ability to:

303 (1) Comply with federal, state, or local laws;

304 (2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or
305 summons by federal, state, or local authorities;

306 (3) Cooperate with law enforcement agencies concerning conduct or activity that the
307 business, service provider, or third party reasonably and in good faith believes may violate
308 federal, state, or local law;

309 (4) Exercise legal rights or privileges; or

310 (5) Engage in news gathering activities protected by the First Amendment.

311 (b) This chapter shall not apply to any of the following:

(1) A business collecting or disclosing personal information of the business’s employees so long as the business is collecting or disclosing such information within the scope of its role as an employer.

(2) Health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services in 45 C.F.R. parts 160 and 164, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 and the federal Health Information Technology for Economic and Clinical Health Act.

(3) A covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services in 45 C.F.R. parts 160 and 164, established pursuant to the federal Health Insurance Portability and Accountability Act of 1996, to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (2) of this section.

(4) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(5) Sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a “consumer report” as defined by 15 U.S.C. section 1681(a) and use of that information is limited by the federal Fair Credit Reporting Act, 15 U.S.C. section 1681 et seq..

(6) Personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, 12 U.S.C. section 24(a) et seq. and implementing regulations.

(7) Personal information collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. section 2721 et seq.;

(8) Education information covered by the federal Family Educational Rights and Privacy Act, 20 U.S.C. section 1232g and 34 C.F.R. part 99.

Section 9. Private Right of Action.

(a) A consumer who has suffered a violation of this chapter may bring a lawsuit against the business or service provider that violated this chapter. A violation of this chapter shall constitute an injury in fact to the consumer who has suffered the violation, and the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation of this chapter.

(b) A consumer who prevails in such a lawsuit shall be entitled to the following remedies:

(1) Damages in an amount not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater;

(2) Injunctive or declaratory relief, as the court deems proper;

(3) Reasonable attorney fees and costs; and

(4) Any other relief the court deems proper.

(c) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not

limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(d) Upon commencement of any action brought under this section, the clerk of the court shall mail a copy of the bill in equity to the attorney general and, upon entry of any judgment or decree in the action, the clerk of the court shall mail a copy of such judgment or decree to the attorney general.

Section 10. Attorney General Enforcement

(a) Whenever the attorney general has reason to believe that any business, service provider, or other person is in violation of this chapter, and that proceedings would be in the public interest, the attorney general may bring an action in the name of the commonwealth against such person to restrain such violation by temporary restraining order or preliminary or permanent injunction. In addition, the attorney general, in an action in the name of the commonwealth, may seek a civil penalty of not more than \$2,500 for each violation or \$7,500 for each intentional violation.

(b) A business that discloses personal information to a service provider shall not be liable under this chapter if the service provider receiving the personal information uses it in violation of the restrictions set forth in this chapter, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this chapter for the obligations of a business for which it provides services as set forth in this chapter.

Section 11. Attorney General Regulations.

(a) On or before July 1, 2022, the attorney general shall solicit broad public participation and adopt regulations to further the purposes of this chapter, including, but not limited to, the following areas:

(1) Updating as needed additional categories of personal information to those enumerated in subdivision (o) of section 1 and subdivision (b) of section 8 in order to address changes in technology, data collection practices, obstacles to implementation and privacy concerns.

(2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation and privacy concerns.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of verifiable consumer requests pursuant to sections 3 through 6.

(B) To govern business and service provider's response to verifiable consumer requests pursuant to sections 3 through 6.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out third party disclosure of consumer personal information.

(5) Adjusting the monetary threshold in subparagraph (C) of paragraph (1) of subdivision (c) of section 1 in January of every odd-numbered year to reflect any increase in the United States Bureau of Labor Statistics' Consumer Price Index.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this chapter are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this chapter and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of sections 3 through 6, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity.

(b) The attorney general may adopt additional regulations as necessary to further the purposes of this chapter and may update an regulations promulgated pursuant to this chapter as needed.

(c) The attorney general shall not bring an enforcement action under this chapter until six months after the publication of the final regulations issued pursuant to this section.

Section 12. Harmony with Other Laws.

Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this chapter, but in the event of a conflict between other laws and the provisions of this chapter, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

Section 13. Evasion.

If a series of steps or transactions where component parts of a single transaction were taken with the intention of avoiding the reach of this chapter, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this chapter.

Section 14. Rights are Non-Waivable.

Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this chapter, including, but not limited to, any right to a remedy or means of enforcement, shall be considered contrary to public policy and shall be void and unenforceable.

SECTION 2. This act shall take effect January 1, 2023.