

SENATE No. 46

The Commonwealth of Massachusetts

PRESENTED BY:

Cynthia Stone Creem

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

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

An Act establishing the Massachusetts Information Privacy Act.

PETITION OF:

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

SENATE No. 46

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

The Commonwealth of Massachusetts

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

An Act establishing the Massachusetts Information Privacy Act.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

1 SECTION 1. The General Laws, as appearing in the 2018 Official Edition, are hereby
2 amended by inserting after chapter 93K the following chapter:

3 CHAPTER 93L. Massachusetts Information Privacy Act

4 Section 1. Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

64 “Data processor” means a person or entity that processes personal information on behalf
65 of a covered entity.

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

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

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

76 “Entity” means the following entities as defined in section 1.40 of chapter 156D:

77 i. “Corporation”, “domestic corporation” or “domestic business corporation”;

78 ii. “Other entity”; and

79 iii. “Foreign business corporation” or “foreign other entity”.

80 This term does not include Massachusetts governmental entities.

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

83 i. Direct or indirect financial harm;

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

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

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

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

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

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

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

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

103 “Individual” means a natural person who is a resident of the Commonwealth of
104 Massachusetts. The location of a natural person in the Commonwealth of Massachusetts shall
105 create a presumption that the natural person is a Commonwealth of Massachusetts resident.

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

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

112 i. IP addresses;

113 ii. GPS coordinates;

114 iii. Cell-site location information;

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

117 v. Information derived from transportation cards;

118 vi. Information related to an individual’s visit to certain locations.

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

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

129 “Person” means any natural or legal person.

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

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

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

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

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

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

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

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

148 vii. Biometric information;

149 viii. Location information;

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

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

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

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

158 xiii. Browser personal information;

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

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

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

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

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

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

173 ii. Date of birth;

- 174 iii. Cellphone number;
- 175 iv. Information revealing political opinions, religious or philosophical beliefs held by
176 identified individuals;
- 177 v. Biometric information;
- 178 vi. Location information;
- 179 vii. Medical and health information including an individual’s medical history and
180 search queries related to medical conditions;
- 181 viii. Information pertaining to an individual’s sex life;
- 182 ix. Social security number; and
- 183 x. Credit scores related to the financial capacity of an individual.

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

191 “Third-party” means, with respect to an individual’s personal information, any person or
192 governmental entity that is not the covered entity or a data processor.

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

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

200 Section 2. General principles and duties

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

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

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

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

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

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

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

215 1. benefits themselves to the detriment of an individual;

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

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

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

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

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

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

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

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

235 (a) Access to and Portability of Personal Information

236 1. Individuals shall have the right to:—

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

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

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

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

245 3. the purposes of the processing;

246 4. the categories of personal information concerned;

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

249 6. the period of retention of the personal information.

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

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

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

256 (b) Correction and Deletion of Personal Information

257 1. Individuals shall have the right to:—

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

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

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

265 (c) Exercise of Rights

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

268 i. clear and conspicuous;

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

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

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

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

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

281 Section 4. Right to know

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

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

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

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

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

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

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

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

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

305 ii. be clear and prominent in appearance;

306 iii. use clear and plain language;

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

309 v. be reasonably understandable;

- 310 vi. be distinguishable from other matters;
- 311 vii. not contain any unrelated, confusing, or contradictory information;
- 312 viii. be no more than 600 words, excluding the list of third parties with which the
313 covered entity discloses personal information; and
- 314 ix. be provided free of charge.
- 315 5. The short-form privacy notice required must include:—
- 316 i. the sensitive personal information being processed;
- 317 ii. the use model and a brief explanation of the relationship between the individual
318 and the covered entity;
- 319 iii. whether the covered entity by itself or a data processor on its behalf processes the
320 information;
- 321 iv. whether the covered entity uses automated decision systems;
- 322 v. whether personal information is going to be processed for purposes of targeted
323 advertisement or monetization;
- 324 vi. one example of harm that may arise from a misuse of the personal information;
- 325 vii. the period of retention of the personal information expressed in exact dates;
- 326 viii. to what types of third parties the covered entity discloses personal information
327 and for what purposes, including governmental entities; and

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

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

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

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

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

343 8. The commission shall:—

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

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

- 348 iii. develop a recognizable and uniform logo or button to promote individual
349 awareness of the short-form privacy notice; and
- 350 iv. promulgate regulations specifying additional requirements for the format and
351 substance of short-form privacy notices.

352 Section 5. Right to consent

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

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

358 1. A covered entity must obtain consent:—

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

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

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

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

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

370 3. A covered entity requesting consent shall:—

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

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

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

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

379 i. threaten or mandate an individual's compliance;

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

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

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

385 v. deliberately increase work for the individual;

- 386 vi. interrupt the individual’s task flow;
- 387 vii. use information architectures and navigation mechanisms that guide the
- 388 individual toward not having a real option to consent;
- 389 viii. hide desired content or interface elements;
- 390 ix. limit or omit controls that would facilitate task accomplishment by the individual;
- 391 x. present disturbing content to the individual; or
- 392 xi. generally mislead or deceive the individual.

393 5. Once an individual refuses to provide consent in accordance with this section, and

394 if the individual keeps interacting with the covered entity in any way, the covered entity shall not

395 try to obtain consent unless a period of at least six months has passed.

396 6. Under no circumstances shall the mere covered interaction of an individual with a

397 covered entity’s product or service be deemed as consent.

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

399 covered entity:—

- 400 i. processes only the personal information necessary to request consent;
- 401 ii. processes such information solely to request consent; and
- 402 iii. immediately deletes all the personal information if consent is refused.

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

406 8. A covered entity shall not:—

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

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

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

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

420 Section 6. Right to control disclosure of personal information

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

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

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

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

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

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

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

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

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

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

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

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

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

450 i. limit the violator’s access to personal information;

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

453 iii. notify the commission about the violation.

454 Section 7. Prohibition of surreptitious surveillance

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

463 Section 8. Age of responsibility

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

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

469 Section 9. Protection of biometric and location information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

519 Section 10. Prohibition of discrimination

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

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

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

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

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

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

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

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

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

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

550 Section 11. Prohibition of unfair and deceptive trade practices

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

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

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

557 2. take unreasonable advantage of:—

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

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

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

564 Section 12. The Massachusetts information privacy commission

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

- 567 1. appoint officers and hire employees;
- 568 2. establish and amend a plan of organization that it considers expedient;
- 569 3. execute all instruments necessary or convenient for accomplishing the purposes of
570 this chapter and its regulation;
- 571 4. adopt, amend, or repeal regulations for the implementation, administration, and
572 enforcement of this chapter.
- 573 5. enter into agreements or other transactions with a person, including, but not
574 limited to, a governmental entity or other governmental instrumentality or authority in
575 connection with its powers and duties under this chapter;
- 576 6. appear on its own behalf before boards, commissions, departments, or other
577 agencies of municipal, state, or federal government;
- 578 7. apply for and accept subventions, grants, loans, advances, and contributions of
579 money, property, labor, or other things of value from any source, to be held, used, and applied
580 for its purposes;
- 581 8. provide and pay for advisory services and technical assistance as may be
582 necessary for its judgment to carry out this chapter and fix the compensation of persons
583 providing such services or assistance;
- 584 9. prepare, publish and distribute, with or without charge as the commission may
585 determine, such studies, reports, bulletins, and other materials as the commission considers
586 appropriate;

- 587 10. gather facts and information applicable to the commission’s obligation to enforce
588 this chapter and ensure its compliance;
- 589 11. conduct investigations for possible violations of this chapter;
- 590 12. conduct adjudicatory proceedings and promulgate regulations in accordance with
591 chapter 30A;
- 592 13. refer cases for criminal prosecution to the appropriate federal, state, or local
593 authorities;
- 594 14. maintain an official internet website for the commission.
- 595 15. conduct a study to determine the most effective way for covered entities to obtain
596 individuals’ consent in accordance with section 5 for each type of personal information
597 processing.
- 598 i. The commission may request data and information from covered entities
599 conducting business in Massachusetts, Massachusetts government entities administering notice
600 and consent regimes, consumer protection experts, privacy advocates, and researchers, Internet
601 standards-setting bodies such as the Internet Engineering Taskforce and Institute of Electrical
602 and Electronics Engineers, and other relevant sources to meet the purpose of the study.
- 603 16. assess and impose civil administrative penalties on covered entities, data
604 processors, and third parties who fail to comply with or violate any provision of this chapter or
605 regulation enacted pursuant to this chapter, and create an administrative procedure for such
606 purpose.; and

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

609 Section 13. Enforcement – Civil administrative penalties.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 685 1. less than 0.15% of the annual global revenue of the covered entity, data processor,
686 or third-party or \$15,000, whichever is greater, per individual violation; or
- 687 2. more than 4% of the covered entity's annual global revenue, data processor, or
688 third-party or \$20,000,000, whichever is greater, if the commission assesses a civil
689 administrative penalty for multiple violations that affect multiple individuals.

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

- 692 1. the number of affected individuals;
- 693 2. the severity of the violation or noncompliance;

- 694 3. the risks caused by the violation or noncompliance;
- 695 4. whether the violation or noncompliance was part of a pattern of noncompliance
696 and violations and not an isolated instance;
- 697 5. whether the violation or noncompliance was willful and not the result of error;
- 698 6. the precautions taken by the defendant to prevent a violation;
- 699 7. the number of administrative actions, lawsuits, settlements, and consent-decrees
700 under this chapter involving the defendant;
- 701 8. the number of administrative actions, lawsuits, settlements, and consent-decrees
702 involving the defendant in other states and at the federal level in issues involving information
703 privacy; and
- 704 9. the international record of the defendant when it comes to information privacy
705 issues;
- 706 (k) Notwithstanding any general or special law to the contrary, including the
707 limitations and considerations set forth in this section, the commission may require that the
708 amount of a civil administrative penalty imposed pursuant to this section exceeds the economic
709 benefit realized by a person for noncompliance.
- 710 (l) When imposing civil administrative penalties, the commission shall consider the
711 following:—
- 712 1. each individual whose personal information was unlawfully processed, and each
713 instance of processing counts as a separate violation;

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

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

718 (m) All civil administrative penalties assessed shall be paid to the commonwealth.

719 Once the payment is received, the commonwealth shall:—

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

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

724 Section 14. Enforcement - Judicial remedies

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

728 1. An individual protected by this chapter may not be required, as a condition of
729 service or otherwise, to file an administrative complaint with the commission or to accept
730 mandatory arbitration of a claim under this chapter.

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

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

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

737 i. liquidated damages of not less than 0.15% of the annual global revenue of the
738 covered entity or \$15,000 per violation, whichever is greater;

739 ii. punitive damages; and

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

742 5. In addition to any relief awarded pursuant to the previous paragraph, the court
743 shall award reasonable attorney’s fees and costs to any prevailing plaintiff.

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

745 (b) The attorney general may bring an action pursuant to section 4 of chapter 93A
746 against a covered entity, data processor, or third-party to remedy violations of this chapter and
747 for other relief that may be appropriate.

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

751 i. not less than 0.15% of the annual global revenue or \$15,000, whichever is greater,
752 per violation; and

753 ii. not more than 4% of the annual global revenue of the covered entity, data
754 processor, or third-party or \$20,000,000, whichever is greater, per action if such action includes
755 multiple violations to multiple individuals;

756 2. During the proceedings, the court may also request the opinion of the commission
757 on the matters discussed.

758 3. All money awards shall be paid to the commonwealth. The commonwealth shall
759 identify the individuals affected by the violation and earmark such money awards, penalties, or
760 assessments collected for purposes of paying for the damages they suffered as a consequence of
761 the violation.

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

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

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

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

771 Section 15. Enforcement - Miscellaneous

772 (a) Non-waivable rights. Any provision of a contract or agreement of any kind,
773 including a covered entity's terms of service or a privacy policy, including the short-form

774 privacy notice required under section 4 that purports to waive or limit in any way an individual's
775 rights under this chapter, including but not limited to any right to a remedy or means of
776 enforcement shall be deemed contrary to public policy and shall be void and unenforceable.

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

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

784 Section 16. Exceptions

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

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

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

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

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

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

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

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

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

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

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

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

814 v. not attempt to re-identify the information.

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

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

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

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

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

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

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

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

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

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

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

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

842 Section 17. Transparency

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

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

848 i. The total number of legal requests, disaggregated by type of requests such as
849 warrants, court orders, and subpoenas.

850 ii. The number of legal requests that resulted in the covered entity disclosing
851 personal information;

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

854 iv. The type of personal information sought in the legal requests received by the
855 covered entity; and

856 v. The total number of legal requests seeking the disclosure of location or biometric
857 information;

858 vi. The number of legal requests that resulted in the covered entity disclosing
859 location or biometric information;

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

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

864 2. take all reasonable measures and engage in all legal actions available to ensure
865 that the legal request is valid under applicable laws and statutes; and

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

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

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

872 i. applicable law or statute that mandates such disclosure;

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

874 iii. the type of personal information disclosed.

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

877 (c) The commission shall:—

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

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

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

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

885 Section 18. Non-applicability

886 (a) This chapter shall not apply to:

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

895 2. individuals sharing their personal contact information such as email addresses
896 with other individuals in the workplace, or other social, political, or similar settings where the
897 purpose of the information is to facilitate communication among such individuals, provided that
898 this chapter shall cover any processing of such contact information beyond interpersonal
899 communication.

900 3. covered entities' publication of entity-based member or employee contact
901 information where such publication is intended to allow members of the public to contact such
902 member or employee in the ordinary course of the entity's operations.

903 Section 19. Relationship with other laws

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

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

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

913 Section 20. Severability

914 (a) Should any provision of this chapter or part hereof be held under any
915 circumstances in any jurisdiction to be invalid or unenforceable, such invalidity or

916 unenforceability shall not affect the validity or enforceability of any other provision of this or
917 other parts of this chapter.

918 SECTION 2. Chapter 10 of the General Laws, as appearing in the 2018 Official Edition,
919 is hereby amended by inserting after section 78 the following sections:-

920 Section 79.

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

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

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

- 931 1. information privacy, technology, and the law;
- 932 2. social implications of artificial intelligence and digital equity;
- 933 3. data science and data surveillance; or
- 934 4. digital services, digital markets, and consumer protection of digital data.

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

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

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

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

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

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

965 (i) Commissioners shall receive salaries not greater than $\frac{3}{4}$ of the salary of the
966 secretary of administration and finance under section 4 of chapter 7; provided, however, that the
967 chair shall receive a salary equal to the salary of the secretary of administration and finance.
968 Commissioners shall devote their full time and attention to the duties of their office.

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

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

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

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

992 (m) The commission shall appoint an executive director. The executive director shall
993 serve at the pleasure of the commission, shall receive such salary as may be determined by the
994 commission, and shall devote full time and attention to the duties of the office. The executive
995 director shall be a person with skill and experience in management, shall be the executive and
996 administrative head of the commission, and shall be responsible for administering and enforcing
997 the law relative to the commission and each administrative unit thereof. The executive director
998 shall appoint and employ a chief financial and accounting officer and may, subject to the
999 approval of the commission, employ other employees, consultants, agents, and advisors,
1000 including legal counsel, and shall attend meetings of the commission. The chief financial and
1001 accounting officer of the commission shall be in charge of its funds, books of account, and

1002 accounting records. No funds shall be transferred by the commission without the approval of the
1003 commission and the signatures of the chief financial and accounting officer and the treasurer of
1004 the commission. In the case of an absence or vacancy in the office of the executive director or in
1005 the case of disability, as determined by the commission, the commission may designate an acting
1006 executive director to serve as executive director until the vacancy is filled or the absence or
1007 disability ceases. The acting executive director shall have all of the powers and duties of the
1008 executive director and shall have similar qualifications as the executive director.

1009 (n) Chapters 268A and 268B shall apply to the commissioners and to employees of
1010 the commission; provided, however, that the commission shall establish a code of ethics for all
1011 members and employees that shall be more restrictive than said chapters 268A and 268B. A copy
1012 of the code shall be filed with the state ethics commission. The code shall include provisions
1013 reasonably necessary to carry out the purposes of this section and any other laws subject to the
1014 jurisdiction of the commission including, but not limited to: (i) prohibiting the receipt of gifts by
1015 commissioners and employees from any entity subject to the jurisdiction of the commission; (ii)
1016 prohibiting the participation by commissioners and employees in a particular matter as defined in
1017 section 1 of said chapter 268A that affects the financial interest of a relative within the third
1018 degree of consanguinity or a person with whom such commissioner or employee has a significant
1019 relationship as defined in the code; and (iii) providing for recusal of a commissioner in a decision
1020 due to a potential conflict of interest.

1021 (o) The Massachusetts information privacy commission shall be a commission for the
1022 purposes of section 3 of chapter 12.

1023 (p) The commission shall, for the purposes of compliance with state finance law,
1024 operate as a state agency as defined in section 1 of chapter 29 and shall be subject to the laws
1025 applicable to agencies under the control of the governor; provided, however, that the comptroller
1026 may identify any additional instructions or actions necessary for the commission to manage
1027 fiscal operations in the state accounting system and meet statewide and other governmental
1028 accounting and audit standards. The commission shall properly classify the commission's
1029 operating and capital expenditures and shall not include any salaries of employees in the
1030 commission's capital expenditures. Unless otherwise exempted by law or the applicable central
1031 service agency, the commission shall participate in any other available commonwealth central
1032 services including, but not limited to, the state payroll system pursuant to section 31 of said
1033 chapter 29, and may purchase other goods and services provided by state agencies in accordance
1034 with comptroller provisions. The comptroller may chargeback the commission for the transition
1035 and ongoing costs for participation in the state accounting and payroll systems and may retain
1036 and expend such costs without further appropriation for the purposes of this section. The
1037 commission shall be subject to section 5D and subsection (f) of section 6B of said chapter 29.

1038 (q) The commission shall be subject to chapter 30A.

1039 Section 80.

1040 (a) There shall be an information privacy advisory board to study and make
1041 recommendations to the Massachusetts information privacy commission on issues related to
1042 information privacy in the Commonwealth. The board shall consist of: the executive director of
1043 the Massachusetts information privacy commission who shall serve as chair; the secretary of
1044 technology services and security or the secretary's designee; the house and senate chairs of the

1045 joint committee on state administration and regulatory oversight; the chief justice of the supreme
1046 judicial court or a designee; the attorney general or a designee; the state auditor or a designee;
1047 the inspector general or a designee; the secretaries of the executive office of public safety and
1048 security, department of children and families, and executive office of health and human services,
1049 or their designees; the chief counsel of the committee for public counsel services or a designee;
1050 the chief legal counsel of the Massachusetts Bar Association or a designee; the executive director
1051 of the American Civil Liberties Union of Massachusetts or a designee; 2 academics who shall be
1052 experts in (i) data science, artificial intelligence, and machine learning, (ii) social implications of
1053 artificial intelligence and technology, or (iii) information policy, technology, and the law; 2
1054 academics who shall be experts in (i) artificial intelligence and machine learning, (ii) data
1055 science and information policy, or (iii) technology and the law; the executive director of the
1056 Massachusetts Law Reform Institute or a designee; 1 representative from a the National
1057 Association of Social Workers; and 1 representative from the Massachusetts High Technology
1058 Council. Members of the board shall serve for terms of 2 years. Members of the board shall serve
1059 without compensation but shall be reimbursed for their expenses actually and necessarily
1060 incurred in the discharge of their official duties. Members of the board shall not be state
1061 employees under chapter 268A by virtue of their service on the board. To take action at a
1062 meeting, a majority of the members of the board present and voting shall constitute a quorum.

1063 (b) The information privacy advisory board shall: (i) consider all matters submitted to
1064 it by the commission; (ii) on its own initiative, recommend to the commission guidelines, rules
1065 and regulations and any changes to guidelines, rules, and regulations that the advisory board
1066 considers important or necessary for the commission's review and consideration; and (iii) advise
1067 on the preparation of regulations pursuant to chapter 93L of the general laws.

1068 (c) The chair may appoint subcommittees to expedite the work of the board.

1069 SECTION 3. Section 5 of Chapter 93H of the General Laws, as appearing in the 2020
1070 Official Edition, is hereby amended by inserting after the words “office of consumer affairs and
1071 business regulation” in the two places where those words appear the following:

1072 , and the Massachusetts information privacy commission

1073 SECTION 4. Chapter 149 of the General Laws, as appearing in the 2018 Official Edition,
1074 is hereby amended by inserting after section 203 the following section:

1075 Section 204. Workplace Surveillance

1076 a. For the purposes of this section, the following words shall have the following
1077 meanings unless the context clearly requires otherwise:

1078 “Information” also referred to as “employee information,” or “data” means information
1079 that identifies, relates to, describes, is reasonably capable of being associated with, or could
1080 reasonably be linked, directly or indirectly, with a particular employee, regardless of how the
1081 information is collected, inferred, or obtained.

1082 “Electronic monitoring” means the collection of information concerning employee
1083 activities, communications, actions, biometrics, or behaviors by electronic means.

1084 “Employment-related decision” means any decision made by the employer that affects
1085 wages, benefits, hours, work schedule, performance evaluation, hiring, discipline, promotion,
1086 termination, job content, productivity requirements, workplace health and safety, or any other
1087 terms and conditions of employment.

1088 “Vendor” means a business engaged in a contract with an employer to provide services,
1089 software, or technology that collects, stores, analyzes, or interprets employee information.

1090 “Facial recognition technology” shall have the meaning established in section 220 of
1091 chapter 6 of the General Laws, as amended by Chapter 253 of the Acts of 2020.

1092 b. An employer, or vendor acting on behalf of an employer, shall not electronically
1093 monitor an employee unless:—

1094 1. the electronic monitoring only purpose is to—

1095 i. enable tasks that are necessary to accomplish essential job functions;

1096 ii. monitor production processes or quality;

1097 iii. comply with employment, labor, or other relevant laws;

1098 iv. protect the safety and security of employees; or

1099 v. carry on other purposes as determined by the department of labor standards; and

1100 2. the specific form of electronic monitoring is:—

1101 i. necessary to accomplish the allowable purpose;

1102 ii. the least invasive means that could reasonably be used to accomplish the
1103 allowable purpose;

1104 iii. limited to the smallest number of employees; and

1105 iv. collecting the least amount of information necessary to accomplish the purpose
1106 mentioned in (1).

- 1107 c. Notwithstanding subsection (b), the following practices shall be prohibited:—
- 1108 1. use of electronic monitoring that either directly or indirectly harms an employee’s
- 1109 physical health, mental health, personal safety or wellbeing;
- 1110 2. monitoring of employees who are off-duty and not performing work-related tasks;
- 1111 3. audio-visual monitoring of bathrooms or other similarly private areas including
- 1112 locker rooms and changing areas;
- 1113 4. audio-visual monitoring of break rooms, lounges, and other social spaces, except
- 1114 to investigate specific illegal activity;
- 1115 5. use of facial recognition technology other than for the purpose of verifying the
- 1116 identity of an employee for security purposes; and
- 1117 6. any other forms of electronic monitoring such as may be prohibited by the
- 1118 department of labor standards.
- 1119 d. Employers shall not require employees to install applications on personal or
- 1120 mobile devices that collect employee information or require employees to wear data-collecting
- 1121 devices, including those that are incorporated into items of clothing or personal accessories,
- 1122 unless the electronic monitoring is necessary to accomplish essential job functions and is
- 1123 narrowly limited to only the activities and times necessary to accomplish essential job functions.
- 1124 e. Information resulting from electronic monitoring shall be accessed only by
- 1125 authorized agents and used only for the purpose and duration for which notice was given in
- 1126 accordance with subsection (f).

1127 f. Employers shall provide employees with notice that electronic monitoring will
1128 occur prior to conducting each specific form of electronic monitoring. The notice must, at a
1129 minimum, include:—

1130 1. a description of—

1131 i. the purpose that the specific form of electronic monitoring is intended to
1132 accomplish, as specified in subsection (b);

1133 ii. the specific activities, locations, communications, and job roles that will be
1134 electronically monitored;

1135 iii. the technologies used to conduct the specific form of electronic monitoring;

1136 iv. the vendors or other third parties that information collected through electronic
1137 monitoring will be disclosed or transferred to, including the name of the vendor and the purpose
1138 for the data transfer;

1139 v. the organizational positions that are authorized to access the information collected
1140 through the specific form of electronic monitoring, and under what conditions; and

1141 vi. the dates, times, and frequency that electronic monitoring will occur.

1142 2. the names of any vendors conducting electronic monitoring on the employer’s
1143 behalf; and

1144 3. an explanation of:—

1145 i. the reasons why the specific form of electronic monitoring is necessary to
1146 accomplish the purpose; and

1147 ii. how the specific monitoring practice is the least invasive means available to
1148 accomplish the allowable monitoring purpose.

1149 g. The notice mentioned in (f) shall be clear and conspicuous and provide the
1150 employee with actual notice of electronic monitoring activities.

1151 1. A notice that provides electronic monitoring "may" take place or that the
1152 employer "reserves the right" to monitor shall not suffice.

1153 h. An employer who engages in random or periodic electronic monitoring of
1154 employees will inform the affected employees of the specific events which are being monitored
1155 at the time the monitoring takes place with a notice that shall be clear and conspicuous.

1156 1. Notwithstanding the previous paragraph, notice of random or periodic electronic
1157 monitoring may be given after electronic monitoring has occurred only if necessary to preserve
1158 the integrity of an investigation of wrongdoing or protect the immediate safety of employees,
1159 customers, or the public.

1160 i. Employers shall provide a copy of the above notice disclosure to the department
1161 of labor standards.

1162 j. An employer shall only use employee information collected through electronic
1163 monitoring to accomplish its purpose, unless the information documents illegal activity.

1164 k. When making a hiring or employment-related decision using information
1165 collected through electronic monitoring, an employer shall:-

1166 1. not make the decision based solely on such information;

1167 2. give the affected employee access to the data and provide an opportunity to
1168 correct or explain it;

1169 3. corroborate such information by other means, such as independent documentation
1170 by supervisors or managers, or by consultation with other employees; and

1171 4. document and communicate to affected employees the basis for the corroboration
1172 prior to the decision going into effect.

1173 1. Subsection (k) shall not apply to those cases when electronic monitoring data
1174 provides evidence of illegal activity.

1175 SECTION 5. Effective date

1176 (a) Section 2 shall take effect immediately.

1177 (b) The remaining sections shall take effect 12 months after this Act is enacted.

1178 (c) The enforcement of chapter 93L shall be delayed until 18 months after this Act is
1179 enacted.