

**SENATE . . . . . No. 25**

---

**The Commonwealth of Massachusetts**

PRESENTED BY:

*Cynthia Stone Creem*

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

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

An Act establishing the Massachusetts Data Privacy Protection Act.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	
<i>Cynthia Stone Creem</i>	<i>Norfolk and Middlesex</i>	
<i>Jason M. Lewis</i>	<i>Fifth Middlesex</i>	<i>2/9/2023</i>
<i>Patrick M. O'Connor</i>	<i>First Plymouth and Norfolk</i>	<i>10/12/2023</i>
<i>Michael O. Moore</i>	<i>Second Worcester</i>	<i>12/27/2023</i>

**SENATE . . . . . No. 25**

---

---

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

---

---

**The Commonwealth of Massachusetts**

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

An Act establishing the Massachusetts Data Privacy Protection Act.

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

1           SECTION 1. The General Laws, as appearing in the 2020 Official Edition, are hereby  
2 amended by inserting after chapter 93K the following chapter:

3           Chapter 93L. Massachusetts Data Privacy Protection 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           (1)“affirmative express consent”, an affirmative act by an individual that clearly  
8 communicates the individual’s freely given, specific, and unambiguous authorization for an act  
9 or practice after having been informed, in response to a specific request from a covered entity  
10 that meets the requirements of this chapter.

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

12 (3)“biometric information”, any covered data generated from the technological  
13 processing of an individual’s unique biological, physical, or physiological characteristics that is  
14 linked or reasonably linkable to an individual, including:—

15 (i)fingerprints;

16 (ii)voice prints;

17 (iii)iris or retina scans;

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

19 (v)gait or personally identifying physical movements.

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

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

25 (5)“control”, with respect to an entity:—

26 (i)ownership of, or the power to vote, more than 50 percent of the outstanding shares of  
27 any class of voting security of the entity;

28 (ii)control over the election of a majority of the directors of the entity (or of individuals  
29 exercising similar functions); or

30 (iii)the power to exercise a controlling influence over the management of the entity.

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

37 (7) “covered data”, information, including derived data and unique persistent  
38 identifiers, that identifies or is linked or reasonably linkable, alone or in combination with other  
39 information, to an individual or a device that identifies or is linked or reasonably linkable to an  
40 individual. The term “covered data” does not include:—

41 (i)de-identified data;

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

43 (iii)publicly available information.

44 (8)“covered entity”, any entity or any person, other than an individual acting in a non-  
45 commercial context, that alone or jointly with others determines the purposes and means of  
46 collecting, processing, or transferring covered data. The term “covered entity” does not  
47 include:—

48 (i)government agencies or service providers to government agencies that exclusively and  
49 solely process information provided by government entities;

50 (ii)any entity or person that meets the following criteria for the period of the 3 preceding  
51 calendar years (or for the period during which the covered entity or service provider has been in  
52 existence if such period is less than 3 years):—

53 (A)the entity or person’s average annual gross revenues during the period did not exceed  
54 \$20,000,000;

55 (B)the entity or person, on average, did not annually collect or process the covered data  
56 of more than 75,000 individuals during the period beyond the purpose of initiating, rendering,  
57 billing for, finalizing, completing, or otherwise collecting payment for a requested service or  
58 product, so long as all covered data for such purpose was deleted or de-identified within 90 days,  
59 except when necessary to investigate fraud or as consistent with a covered entity’s return policy;  
60 and

61 (C)no component of its revenue comes from transferring covered data during any year (or  
62 part of a year if the covered entity has been in existence for less than 1 year) that occurs during  
63 the period.

64 (9)“covered high-impact social media company”, a covered entity that provides any  
65 internet-accessible platform where—

66 (i)such covered entity generates \$3,000,000,000 or more in annual revenue;

67 (ii)such platform has 300,000,000 or more monthly active users for not fewer than 3 of  
68 the preceding 12 months on the online product or service of such covered entity; and

69 (iii)such platform constitutes an online product or service that is primarily used by users  
70 to access or share, user-generated content.

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

72 (11) “de-identified data”, information that does not identify and is not linked or  
73 reasonably linkable to a distinct individual or a device, regardless of whether the information is  
74 aggregated, and if the covered entity or service provider:—

75 (i)takes technical measures to ensure that the information cannot, at any point, be used to  
76 re-identify any individual or device that identifies or is linked or reasonably linkable to an  
77 individual;

78 (ii)publicly commits in a clear and conspicuous manner:—

79 (A)to process and transfer the information solely in a de-identified form without any  
80 reasonable means for re-identification; and

81 (B)to not attempt to re-identify the information with any individual or device that  
82 identifies or is linked or reasonably linkable to an individual; and

83 (iii)contractually obligates any person or entity that receives the information from the  
84 covered entity or service provider:—

85 (A)to comply with all the provisions of this paragraph with respect to the information;  
86 and

87 (B)to require that such contractual obligations be included contractually in all subsequent  
88 instances for which the data may be received.

89 (12)“derived data”, covered data that is created by the derivation of information, data,  
90 assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or another  
91 source of information or data about an individual or an individual’s device.

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

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

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

102 (i)raw sequence data that results from the sequencing of the complete, or a portion of the,  
103 extracted deoxyribonucleic acid (DNA) of an individual; or

104 (ii)genotypic and phenotypic information that results from analyzing raw sequence data  
105 described in subparagraph (A).

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

108 (17)“knowledge”,

109 (i)with respect to a covered entity that is a covered high-impact social media company,  
110 the entity knew or should have known the individual was a covered minor;

111 (ii)with respect to a covered entity or service provider that is a large data holder, and  
112 otherwise is not a covered high-impact social media company, that the covered entity knew or  
113 acted in willful disregard of the fact that the individual was a covered minor; and

114 (iii)with respect to a covered entity or service provider that does not meet the  
115 requirements of clause (i) or (ii), actual knowledge.

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

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

119 (ii)collected, processed, or transferred the covered data of more than 5,000,000  
120 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals,  
121 excluding covered data collected and processed solely for the purpose of initiating, rendering,  
122 billing for, finalizing, completing, or otherwise collecting payment for a requested product or  
123 service; and the sensitive covered data of more than 200,000 individuals or devices that identify  
124 or are linked or reasonably linkable to 1 or more individuals.

125 The term “large data holder” does not include any instance in which the covered entity or  
126 service provider would qualify as a large data holder solely on the basis of collecting or  
127 processing personal email addresses, personal telephone numbers, or log-in information of an  
128 individual or device to allow the individual or device to log in to an account administered by the  
129 covered entity or service provider.

130 (19)“material”, with respect to an act, practice, or representation of a covered entity  
131 (including a representation made by the covered entity in a privacy policy or similar disclosure to  
132 individuals) involving the collection, processing, or transfer of covered data, that such act,  
133 practice, or representation is likely to affect a reasonable individual’s decision or conduct  
134 regarding a product or service;

135 (20)“location information”, information derived from a device or from interactions  
136 between devices, with or without the knowledge of the user and regardless of the technological  
137 method used, that pertains to or directly or indirectly reveals the present or past geographical  
138 location of an individual or device within the Commonwealth of Massachusetts with sufficient  
139 precision to identify street-level location information within a range of 1,850 feet or less.

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

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

144 (23) “processing purpose”, a reason for which a covered entity or service provider  
145 collects, processes, or transfers covered data that is specific and granular enough for a reasonable  
146 individual to understand the material facts of how and why the covered entity or service provider  
147 collects, processes, or transfers the covered data.

148 (24)“publicly available information”, any information that a covered entity or service  
149 provider has a reasonable basis to believe has been lawfully made available to the general public  
150 from:—

151 (i)federal, state, or local government records, if the covered entity collects, processes, and  
152 transfers such information in accordance with any restrictions or terms of use placed on the  
153 information by the relevant government entity;

154 (ii)widely distributed media;

155 (iii)a website or online service made available to all members of the public, for free or for  
156 a fee, including where all members of the public, for free or for a fee, can log in to the website or  
157 online service;

158 (iv)a disclosure that has been made to the general public as required by federal, state, or  
159 local law; or

160 (v)the visual observation of the physical presence of an individual or a device in a public  
161 place, not including data collected by a device in the individual's possession.

162 For purposes of this paragraph, information from a website or online service is not  
163 available to all members of the public if the individual who made the information available via  
164 the website or online service has restricted the information to a specific audience.

165 The term “publicly available information” does not include:—

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

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

169 (iii) covered data with respect to an individual;

170 (iv)biometric information;

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

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

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

175 (25)“reasonably understandable”, of length and complexity such that an individual with  
176 an eighth-grade reading level, as established by the department of elementary and secondary  
177 education, can read and comprehend.

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

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

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

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

186 (iv)biometric information.

187 (v)genetic information.

188 (vi)location information.

189 (vii) an individual's private communications such as voicemails, emails, texts, direct  
190 messages, or mail, or information identifying the parties to such communications, voice  
191 communications, video communications, and any information that pertains to the transmission of  
192 such communications, including telephone numbers called, telephone numbers from which calls  
193 were placed, the time calls were made, call duration, and location information of the parties to  
194 the call, unless the covered entity or a service provider acting on behalf of the covered entity is  
195 the sender or an intended recipient of the communication. Communications are not private for  
196 purposes of this clause if such communications are made from or to a device provided by an  
197 employer to an employee insofar as such employer provides conspicuous notice that such  
198 employer may access such communications.

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

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

205 (x) calendar information, address book information, phone or text logs, photos, audio  
206 recordings, or videos, maintained for private use by an individual, regardless of whether such  
207 information is stored on the individual's device or is accessible from that device and is backed up  
208 in a separate location. Such information is not sensitive for purposes of this paragraph if such  
209 information is sent from or to a device provided by an employer to an employee insofar as such  
210 employer provides conspicuous notice that it may access such information.

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

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

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

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

221 (xv) information identifying an individual's online activities over time and across  
222 third-party websites or online services.

223 (xvi) any other covered data collected, processed, or transferred for the purpose of  
224 identifying the types of covered data listed in clauses (1) through (16).

225 (27) "service provider", a person or entity that:—

226 (i) collects, processes, or transfers covered data on behalf of, and at the direction of, a  
227 covered entity or a government agency; and

228 (ii) receives covered data from or on behalf of a covered entity or a government agency.

229 A service provider that receives service provider data from another service provider as  
230 permitted under this chapter shall be treated as a service provider under this chapter with respect  
231 to such data.

232 (28)“service provider data”, covered data that is collected or processed by or has been  
233 transferred to a service provider by or on behalf of a covered entity or a government agency or  
234 another service provider for the purpose of allowing the service provider to whom such covered  
235 data is transferred to perform a service or function on behalf of, and at the direction of, such  
236 covered entity or government agency.

237 (29) “small business”, a covered entity or a service provider that meets the following  
238 criteria for the period of the 3 preceding calendar years (or for the period during which the  
239 covered entity or service provider has been in existence if such period is less than 3 years):—

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

242 (ii)the covered entity or service provider, on average, did not annually collect or process  
243 the covered data of more than 200,000 individuals during the period beyond the purpose of  
244 initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a  
245 requested service or product, so long as all covered data for such purpose was deleted or de-  
246 identified within 90 days, except when necessary to investigate fraud or as consistent with a  
247 covered entity’s return policy; and

248 (iii)the covered entity or service provider did not derive more than 50 percent of its  
249 revenue from transferring covered data during any year (or part of a year if the covered entity has  
250 been in existence for less than 1 year) that occurs during the period.

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

256 (31) “targeted advertising”, presenting to an individual or device identified by a unique  
257 identifier, or groups of individuals or devices identified by unique identifiers, an online  
258 advertisement that is selected based on known or predicted preferences, characteristics, or  
259 interests associated with the individual or a device identified by a unique identifier; and does not  
260 include:—

261 (i) advertising or marketing to an individual or an individual’s device in response to the  
262 individual’s specific request for information or feedback;

263 (ii) contextual advertising, which is when an advertisement is displayed based on the  
264 content in which the advertisement appears and does not vary based on who is viewing the  
265 advertisement; or

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

268 (32) “third party”, any person or entity, including a covered entity, that—

269 (i) collects, processes, or transfers covered data and is not a consumer-facing business  
270 with which the individual linked or reasonably linkable to such covered data expects and intends  
271 to interact; and

272 (ii) is not a service provider with respect to such data.

273 This term does not include a person or entity that collects covered data from another  
274 entity if the two entities are related by common ownership or corporate control, but only if a  
275 reasonable consumer's reasonable expectation would be that such entities share information.

276 (33) "data broker", a covered entity whose principal source of revenue is derived from  
277 processing or transferring covered data that the covered entity did not collect directly from the  
278 individuals linked or linkable to the covered data. This term does not include a covered entity  
279 insofar as such entity processes employee data collected by and received from a third party  
280 concerning any individual who is an employee of the third party for the sole purpose of such  
281 third-party providing benefits to the employee. An entity may not be considered to be a data  
282 broker for purposes of this chapter if the entity is acting as a service provider.

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

284 (35) "transfer", to disclose, release, disseminate, make available, license, rent, or share  
285 covered data orally, in writing, electronically, or by any other means.

286 (36) "unique identifier", an identifier to the extent that such identifier is reasonably  
287 linkable to an individual or device that identifies or is linked or reasonably linkable to 1 or more  
288 individuals, including a device identifier, Internet Protocol address, cookie, beacon, pixel tag,  
289 mobile ad identifier, or similar technology, customer number, unique pseudonym, user alias,  
290 telephone number, or other form of persistent or probabilistic identifier that is linked or  
291 reasonably linkable to an individual or device. This term does not include an identifier assigned  
292 by a covered entity for the specific purpose of giving effect to an individual's exercise of  
293 affirmative express consent or opt-outs of the collection, processing, and transfer of covered data

294 pursuant to this chapter or otherwise limiting the collection, processing, or transfer of such  
295 information.

296 (37)“widely distributed media”, information that is available to the general public,  
297 including information from a telephone book or online directory, a television, internet, or radio  
298 program, the news media, or an internet site that is available to the general public on an  
299 unrestricted basis, but does not include an obscene visual depiction, as defined in 18 U.S.C.  
300 section 1460.

## 301 Section 2. Duty of Loyalty

302 (a)A covered entity may not collect, process, or transfer covered data unless the  
303 collection, processing, or transfer is limited to what is reasonably necessary and proportionate to  
304 carry out one of the following purposes:—

305 (1)provide or maintain a specific product or service requested by the individual to whom  
306 the data pertains;

307 (2)initiate, manage, complete a transaction, or fulfill an order for specific products or  
308 services requested by an individual, including any associated routine administrative, operational,  
309 and account-servicing activity such as billing, shipping, delivery, storage, and accounting;

310 (3)authenticate users of a product or service;

311 (4)fulfill a product or service warranty;

312 (5)prevent, detect, protect against, or respond to a security incident. For purposes of this  
313 paragraph, security is defined as network security and physical security and life safety, including  
314 an intrusion or trespass, medical alerts, fire alarms, and access control security;

315 (6)to prevent, detect, protect against, or respond to fraud, harassment, or illegal activity  
316 targeted at or involving the covered entity or its services. For purposes of this paragraph, the  
317 term “illegal activity”, a violation of a federal, state, or local law punishable as a felony or  
318 misdemeanor that can directly harm;

319 (7)comply with a legal obligation imposed by state or federal law, or to investigate,  
320 establish, prepare for, exercise, or defend legal claims involving the covered entity or service  
321 provider;

322 (8)effectuate a product recall pursuant to state or federal law;

323 (9)conduct a public or peer-reviewed scientific, historical, or statistical research project  
324 that:—

325 (i)is in the public interest; and

326 (ii)adheres to all relevant laws and regulations governing such research, including  
327 regulations for the protection of human subjects, or is excluded from criteria of the institutional  
328 review board;

329 (10) deliver a communication that is not an advertisement to an individual, if the  
330 communication is reasonably anticipated by the individual within the context of the individual’s  
331 interactions with the covered entity;

332 (11)deliver a communication at the direction of an individual between such individual  
333 and one or more individuals or entities;

334 (12)ensure the data security and integrity of covered data in accordance with chapter  
335 93H;

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

339 (14)transfer assets to a third party in the context of a merger, acquisition, bankruptcy, or  
340 similar transaction when the third party assumes control, in whole or in part, of the covered  
341 entity's assets, only if the covered entity, in a reasonable time prior to such transfer, provides  
342 each affected individual with:—

343 (i)a notice describing such transfer, including the name of the entity or entities receiving  
344 the individual's covered data and their privacy policies; and

345 (ii)a reasonable opportunity to withdraw any previously given consents related to the  
346 individual's covered data and a reasonable opportunity to request the deletion of the individual's  
347 covered data.

348 (b)A covered entity may, with respect to covered data previously collected in accordance  
349 with the previous subsection, process such data:—

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

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

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

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

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

359 (6)perform inventory management or reasonable network management;

360 (7)protect against spam; or

361 (8)debug or repair errors that impair the functionality of a service or product for which  
362 such data was collected.

363 (c)A covered entity or service provider shall not:—

364 (1) engage in deceptive advertising or marketing with respect to a product or service  
365 offered to an individual; or

366 (2)draw an individual into signing up for or acquiring a product or service through:—

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

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

372 (d)Nothing in this chapter shall be construed or interpreted to:—

373 (1)limit or diminish free speech rights of covered entities guaranteed under the First  
374 Amendment to the Constitution of the United States or under Article 16 of Massachusetts  
375 Declaration of Rights; or

376 (2)imply any purpose that is not enumerated in subsections (a) and (b), when applicable.

377 Section 3. Sensitive covered data.

378 (a)A covered entity or service provider shall not:—

379 (1)collect, process, or transfer a Social Security number, except when necessary to  
380 facilitate an extension of credit, authentication, fraud and identity fraud detection and prevention,  
381 the payment or collection of taxes, the enforcement of a contract between parties, or the  
382 prevention, investigation, or prosecution of fraud or illegal activity, or as otherwise required by  
383 state or federal law;

384 (2)collect or process sensitive covered data, except where such collection or processing is  
385 strictly necessary to provide or maintain a specific product or service requested by the individual  
386 to whom the covered data pertains or is strictly necessary to effect a purpose enumerated in  
387 paragraphs (1), (2), (3), (5), (7), (9), (10), (11), (13), (14) of subsection (a) of section 2, and such  
388 data is only used for that purposes;

389 (3)transfer an individual’s sensitive covered data to a third party, unless:—

390 (i)the transfer is made pursuant to the affirmative express consent of the individual, given  
391 before each specific transfer takes place;

392 (ii)the transfer is necessary to comply with a legal obligation imposed by state or federal  
393 law, so long as such obligation preexisted the collection and previous notice of such obligation  
394 was provided to the individual to whom the data pertains;

395 (iii)the transfer is necessary to prevent an individual from imminent injury where the  
396 covered entity believes in good faith that the individual is at risk of death, serious physical  
397 injury, or serious health risk;

398 (iv)in the case of the transfer of a password, the transfer is necessary to use a designated  
399 password manager or is to a covered entity for the exclusive purpose of identifying passwords  
400 that are being re-used across sites or accounts;

401 (v)in the case of the transfer of genetic information, the transfer is necessary to perform a  
402 medical diagnosis or medical treatment specifically requested by an individual, or to conduct  
403 medical research in accordance with federal and state law; and

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

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

#### 407 Section 4. Consent practices

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

410 (1)The request for affirmative consent should be provided to the individual in a clear and  
411 conspicuous standalone disclosure made through the primary medium used to offer the covered  
412 entity's product or service, or only if the product or service is not offered in a medium that  
413 permits the making of the request under this paragraph, another medium regularly used in  
414 conjunction with the covered entity's product or service;

415 (2)The request includes a description of the processing purpose for which the individual's  
416 consent is sought by:—

417 (i)clearly stating the specific categories of covered data that the covered entity shall  
418 collect, process, and transfer necessary to effectuate the processing purpose; and

419 (ii)including a prominent heading and is reasonably understandable so that an individual  
420 can identify and understand the processing purpose for which consent is sought and the covered  
421 data to be collected, processed, or transferred by the covered entity for such processing purpose;

422 (3)The request clearly explains the individual's applicable rights related to consent;

423 (4)The request is made in a manner reasonably accessible to and usable by individuals  
424 with disabilities;

425 (5)The request is made available to the individual in each covered language in which the  
426 covered entity provides a product or service for which authorization is sought;

427 (6)The option to refuse consent shall be at least as prominent as the option to accept, and  
428 the option to refuse consent shall take the same number of steps or fewer as the option to accept;  
429 and

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

433 (b)A covered entity shall not infer that an individual has provided affirmative express  
434 consent to a practice from the inaction of the individual or the individual's continued use of a  
435 service or product provided by the covered entity.

436 (c)A covered entity shall not obtain or attempt to obtain the affirmative express consent  
437 of an individual through:—

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

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

443 Section 5. Privacy by design

444 (a)A covered entity and a service provider shall establish, implement, and maintain  
445 reasonable policies, practices, and procedures that reflect the role of the covered entity or service  
446 provider in the collection, processing, and transferring of covered data and that:—

447 (1)consider applicable federal and state laws, rules, or regulations related to covered data  
448 the covered entity or service provider collects, processes, or transfers;

449 (2)identify, assess, and mitigate privacy risks related to covered minors;

450 (3)mitigate privacy risks, including substantial privacy risks, related to the products and  
451 services of the covered entity or the service provider, including in the design, development, and  
452 implementation of such products and services, considering the role of the covered entity or  
453 service provider and the information available to it; and

454 (4)implement reasonable training and safeguards within the covered entity and service  
455 provider to promote compliance with all privacy laws applicable to covered data the covered  
456 entity collects, processes, or transfers or covered data the service provider collects, processes, or

457 transfers on behalf of the covered entity and mitigate privacy risks, including substantial privacy  
458 risks, taking into account the role of the covered entity or service provider and the information  
459 available to it.

460 (b)The policies, practices, and procedures established by a covered entity and a service  
461 provider under subsection (a), shall correspond with, as applicable:—

462 (1)the size of the covered entity or the service provider and the nature, scope, and  
463 complexity of the activities engaged in by the covered entity or service provider, including  
464 whether the covered entity or service provider is a large data holder, nonprofit organization,  
465 small business, third party, or data broker, considering the role of the covered entity or service  
466 provider and the information available to it;

467 (2)the sensitivity of the covered data collected, processed, or transferred by the covered  
468 entity or service provider;

469 (3)the volume of covered data collected, processed, or transferred by the covered entity  
470 or service provider;

471 (4)the number of individuals and devices to which the covered data collected, processed,  
472 or transferred by the covered entity or service provider relates; and

473 (5)the cost of implementing such policies, practices, and procedures in relation to the  
474 risks and nature of the covered data.

## 475 Section 6. Pricing

476 (a)A covered entity may not retaliate against an individual for:—

477 (1)exercising any of the rights guaranteed by this chapter, or any regulations promulgated  
478 under this chapter; or

479 (2)refusing to agree to collection or processing of covered data for a separate product or  
480 service, including denying goods or services, charging different prices or rates for goods or  
481 services, or providing a different level of quality of goods or services.

482 (b)Nothing in subsection (a) shall be construed to:—

483 (1)prohibit the relation of the price of a service or the level of service provided to an  
484 individual to the provision, by the individual, of financial information that is necessarily  
485 collected and processed only for the purpose of initiating, rendering, billing for, or collecting  
486 payment for a service or product requested by the individual;

487 (2)prohibit a covered entity from offering a different price, rate, level, quality or selection  
488 of goods or services to an individual, including offering goods or services for no fee, if the  
489 offering is in connection with an individual’s voluntary participation in a bona fide loyalty, ,  
490 rewards, premium features, discount or club card program, provided, that the covered entity may  
491 not sell covered data to a third-party as part of such a program unless:—

492 (i)the sale is reasonably necessary to enable the third party to provide a benefit to which  
493 the consumer is entitled;

494 (ii)the sale of personal data to third parties is clearly disclosed in the terms of the  
495 program; and

496 (iii)the third party uses the personal data only for purposes of facilitating such a benefit to  
497 which the consumer is entitled and does not retain or otherwise use or disclose the personal data  
498 for any other purpose;

499 (3)require a covered entity to provide a bona fide loyalty program that would require the  
500 covered entity to collect, process, or transfer covered data that the covered entity otherwise  
501 would not collect, process, or transfer;

502 (4)prohibit a covered entity from offering a financial incentive or other consideration to  
503 an individual for participation in market research;

504 (5)prohibit a covered entity from offering different types of pricing or functionalities with  
505 respect to a product or service based on an individual's exercise of a right to delete; or

506 (6)prohibit a covered entity from declining to provide a product or service insofar as the  
507 collection and processing of covered data is strictly necessary for such product or service.

508 (c)Notwithstanding the provisions in this subsection, no covered entity may offer  
509 different types of pricing that are unjust, unreasonable, coercive, or usurious in nature.

## 510 Section 7. Privacy policy

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

515 (b)The privacy policy must be provided in a manner that is reasonably accessible to and  
516 usable by individuals with disabilities. The policy shall be made available to the public in each

517 covered language in which the covered entity or service provider provides a product or service  
518 that is subject to the privacy policy; or carries out activities related to such product or service.

519 (c)The privacy policy must include, at a minimum, the following:—

520 (1)The identity and the contact information of:—

521 (i)the covered entity or service provider to which the privacy policy applies, including the  
522 covered entity’s or service provider’s points of contact and generic electronic mail addresses, as  
523 applicable for privacy and data security inquiries;

524 (ii)any other entity within the same corporate structure as the covered entity or service  
525 provider to which covered data is transferred by the covered entity;

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

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

530 (v)whether the covered entity or service provider transfers covered data and, if so, each  
531 category of service provider and third party to which the covered entity or service provider  
532 transfers covered data, the name of each data broker to which the covered entity or service  
533 provider transfers covered data, and the purposes for which such data is transferred to such  
534 categories of service providers and third parties or third-party collecting entities, except for a  
535 transfer to a governmental entity pursuant to a court order or law that prohibits the covered entity  
536 or service provider from disclosing such transfer;

537 (vi)The length of time the covered entity or service provider intends to retain each  
538 category of covered data, including sensitive covered data, or, if it is not possible to identify that  
539 timeframe, the criteria used to determine the length of time the covered entity or service provider  
540 intends to retain categories of covered data;

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

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

545 (ix)The effective date of the privacy policy.

546 (d)If a covered entity makes a material change to its privacy policy or practices, the  
547 covered entity shall notify each individual affected by such material change before implementing  
548 the material change with respect to any prospectively collected covered data and, except as  
549 provided in paragraphs (1) through (15) of section 2, provide a reasonable opportunity for each  
550 individual to withdraw consent to any further materially different collection, processing, or  
551 transfer of previously collected covered data under the changed policy.

552 (e)The covered entity shall take all reasonable electronic measures to provide direct  
553 notification regarding material changes to the privacy policy to each affected individual, in each  
554 covered language in which the privacy policy is made available, and taking into account  
555 available technology and the nature of the relationship.

556 (f)Nothing in this section shall be construed to affect the requirements for covered  
557 entities under other sections of this chapter.

558 (g)Each large data holder shall retain copies of previous versions of its privacy policy for  
559 at least 10 years beginning after the date of enactment of this chapter and publish them on its  
560 website. Such large data holder shall make publicly available, in a clear, conspicuous, and  
561 readily accessible manner, a log describing the date and nature of each material change to its  
562 privacy policy over the past 10 years. The descriptions shall be sufficient for a reasonable  
563 individual to understand the material effect of each material change. The obligations in this  
564 paragraph shall not apply to any previous versions of a large data holder’s privacy policy, or any  
565 material changes to such policy, that precede the date of enactment of this Act.

566 (h)In addition to the privacy policy required under subsection (a), a large data holder that  
567 is a covered entity shall provide a short form notice of no more than 500 words in length that  
568 includes the main features of their data practices.

569 Section 8. Individual data rights

570 (a)A covered entity shall provide an individual, after receiving a verified request from the  
571 individual, with the right to:—

572 (1)access:—

573 (i)in a human-readable format that a reasonable individual can understand and download  
574 from the internet, the covered data (except covered data in a back-up or archival system) of the  
575 individual making the request that is collected, processed, or transferred by the covered entity or  
576 any service provider of the covered entity within the 24 months preceding the request;

577 (ii)the categories of any third party, if applicable, and an option for consumers to obtain  
578 the names of any such third party as well as and the categories of any service providers to whom

579 the covered entity has transferred for consideration the covered data of the individual, as well as  
580 the categories of sources from which the covered data was collected; and

581 (iii) a description of the purpose for which the covered entity transferred the covered data  
582 of the individual to a third party or service provider;

583 (2) correct any verifiable substantial inaccuracy or substantially incomplete information  
584 with respect to the covered data of the individual that is processed by the covered entity and  
585 instruct the covered entity to make reasonable efforts to notify all third parties or service  
586 providers to which the covered entity transferred such covered data of the corrected information;

587 (3) delete covered data of the individual that is processed by the covered entity and  
588 instruct the covered entity to make reasonable efforts to notify all third parties or service  
589 provider to which the covered entity transferred such covered data of the individual's deletion  
590 request; and

591 (4) to the extent technically feasible, export to the individual or directly to another entity  
592 the covered data of the individual that is processed by the covered entity, including inferences  
593 linked or reasonably linkable to the individual but not including other derived data, without  
594 licensing restrictions that limit such transfers in:—

595 (i) a human-readable format that a reasonable individual can understand and download  
596 from the internet; and

597 (ii) a portable, structured, interoperable, and machine-readable format.

598 (b) A covered entity may not condition, effectively condition, attempt to condition, or  
599 attempt to effectively condition the exercise of a right described in subsection (a) through:—

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

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

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

608 (d)A response period set forth in this subsection may be extended once by 20 additional  
609 days when reasonably necessary, considering the complexity and number of the individual’s  
610 requests, so long as the covered entity informs the individual of any such extension within the  
611 initial 30-day response period, together with the reason for the extension.

612 (e)A covered entity:—

613 (1)shall provide an individual with the opportunity to exercise each of the rights  
614 described in subsection (a) and with respect to:—

615 (A)the first two times that an individual exercises any right described in subsection (a) in  
616 any 12-month period, shall allow the individual to exercise such right free of charge; and

617 (B)any time beyond the initial two times described in subparagraph (A), may allow the  
618 individual to exercise such right for a reasonable fee for each request.

619 (f)A covered entity may not permit an individual to exercise a right described in  
620 subsection (a), in whole or in part, if the covered entity:—

621 (1)cannot reasonably verify that the individual making the request to exercise the right is  
622 the individual whose covered data is the subject of the request or an individual authorized to  
623 make such a request on the individual’s behalf;

624 (2)reasonably believes that the request is made to interfere with a contract between the  
625 covered entity and another individual;

626 (3)determines that the exercise of the right would require access to or correction of  
627 another individual’s sensitive covered data;

628 (4)reasonably believes that the exercise of the right would require the covered entity to  
629 engage in an unfair or deceptive practice under state law; or

630 (5)reasonably believes that the request is made to further fraud, support criminal activity,  
631 or the exercise of the right presents a data security threat.

632 (g)If a covered entity cannot reasonably verify that a request to exercise a right described  
633 in subsection (a) is made by the individual whose covered data is the subject of the request (or an  
634 individual authorized to make such a request on the individual’s behalf), the covered entity:—

635 (1)may request that the individual making the request to exercise the right provide any  
636 additional information necessary for the sole purpose of verifying the identity of the individual;  
637 and

638 (2)may not process or transfer such additional information for any other purpose.

639 (h)A covered entity may decline, with adequate explanation to the individual, to comply  
640 with a request to exercise a right described in subsection (a), in whole or in part, that would:—

641 (1)require the covered entity to retain any covered data collected for a single, one-time  
642 transaction, if such covered data is not processed or transferred by the covered entity for any  
643 purpose other than completing such transaction;

644 (2)be demonstrably impracticable or prohibitively costly to comply with, and the covered  
645 entity shall provide a description to the requestor detailing the inability to comply with the  
646 request;

647 (3)require the covered entity to attempt to re-identify de-identified data;

648 (4)require the covered entity to maintain covered data in an identifiable form or collect,  
649 retain, or access any data in order to be capable of associating a verified individual request with  
650 covered data of such individual;

651 (5)result in the release of trade secrets or other privileged or confidential business  
652 information;

653 (6)require the covered entity to correct any covered data that cannot be reasonably  
654 verified as being inaccurate or incomplete;

655 (7)interfere with law enforcement, judicial proceedings, investigations, or reasonable  
656 efforts to guard against, detect, prevent, or investigate fraudulent, malicious, or unlawful activity,  
657 or enforce valid contracts;

658 (8)violate state or federal law or the rights and freedoms of another individual, including  
659 under the Constitution of the United States and Massachusetts Declaration of Rights;

660 (9)prevent a covered entity from being able to maintain a confidential record of deletion  
661 requests, maintained solely for the purpose of preventing covered data of an individual from

662 being recollected after the individual submitted a deletion request and requested that the covered  
663 entity no longer collect, process, or transfer such data; or

664 (10) endanger the source of the data if such data could only have been obtained from a  
665 single identified source.

666 (i) A covered entity may decline, with adequate explanation to the individual, to comply  
667 with a request for deletion pursuant to paragraph (3) of subsection (a) if such request:—

668 (1) unreasonably interfere with the provision of products or services by the covered entity  
669 to another person it currently serves;

670 (2) requests to delete covered data that relates to (A) a public figure, public official, or  
671 limited-purpose public figure; or (B) any other individual that has no reasonable expectation of  
672 privacy with respect to such data;

673 (3) requests to delete covered data reasonably necessary to perform a contract between the  
674 covered entity and the individual;

675 (4) requests to delete covered data that the covered entity needs to retain in order to  
676 comply with professional ethical obligations;

677 (5) requests to delete covered data that the covered entity reasonably believes may be  
678 evidence of unlawful activity or an abuse of the covered entity's products or service; or

679 (6) involves private elementary and secondary schools as defined by state law and private  
680 institutions of higher education as defined by title I of the Higher Education Act of 1965 and  
681 targets covered data that would unreasonably interfere with the provision of education services  
682 by or the ordinary operation of the school or institution.

683 (j) In a circumstance that would allow a denial pursuant to this section, a covered entity  
684 shall partially comply with the remainder of the request if it is possible and not unduly  
685 burdensome to do so.

686 (k) The receipt of a large number of verified requests, on its own, may not be considered  
687 to render compliance with a request demonstrably impracticable.

688 (l) A covered entity shall facilitate the ability of individuals to make requests under  
689 subsection (a) in any covered language in which the covered entity provides a product or service.  
690 The mechanisms by which a covered entity enables individuals to make requests under  
691 subsection (a) shall be readily accessible and usable by individuals with disabilities.

## 692 Section 9. Advanced data rights.

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

696 (b) Right to opt-out of covered data transfers. A covered entity:—

697 (1) may not transfer or direct the transfer of the covered data of an individual to a third  
698 party if the individual objects to the transfer; and

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

701 (c) Right to opt out of targeted advertising. A covered entity or service provider that  
702 directly delivers a targeted advertisement shall:—

703 (1) prior to engaging in targeted advertising to an individual or device and at all times,  
704 thereafter, provide such individual with a clear and conspicuous means to opt out of targeted  
705 advertising;

706 (2) abide by any opt-out designation by an individual with respect to targeted advertising  
707 and notify the covered entity that directed the service provider to deliver the targeted  
708 advertisement of the opt-out decision; and

709 (3) allow an individual to make an opt-out designation with respect to targeted advertising  
710 through an opt-out mechanism.

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

715 (e) A covered entity may not condition, effectively condition, attempt to condition, or  
716 attempt to effectively condition the exercise of any individual right under this section through:—

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

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

722 (f) A covered entity shall notify third parties who had access to an individual's covered  
723 data when the individual exercises any of the rights established in this section. The third party

724 shall comply with the request to opt-out of sale or data transfer forwarded to them from a  
725 covered entity that provided, made available, or authorized the collection of the individual's  
726 covered data. The third party shall comply with the request in the same way a covered entity is  
727 required to comply with the request. The third party shall no longer retain, use, or disclose the  
728 personal information unless the third party becomes a service provider or a covered entity in the  
729 terms of this chapter.

730 Section 10. Minors

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

733 Section 11. Data Brokers

734 (a) Each data broker shall place a clear, conspicuous, not misleading, and readily  
735 accessible notice on the website or mobile application of the data broker (if the data broker  
736 maintains such a website or mobile application) that:—

737 (1) notifies individuals that the entity is a data broker;

738 (2) includes a link to the data broker registry website; and

739 (3) is reasonably accessible to and usable by individuals with disabilities.

740 (b) Data broker registration. Not later than January 31 of each calendar year that follows a  
741 calendar year during which a covered entity acted as a data broker, data brokers shall register  
742 with the OCABR in accordance with this subsection.

743 (1) In registering with the OCABR, a data broker shall do the following:—

744 (i) Pay to the OCABR a registration fee of \$100;

745 (ii) Provide the OCABR with the following information:—

746 (A) The legal name and primary physical, email, and internet addresses of the data broker;

747 (B) A description of the categories of covered data the data broker processes and

748 transfers;

749 (C) The contact information of the data broker, including a contact person, a telephone

750 number, an e-mail address, a website, and a physical mailing address; and

751 (D) A link to a website through which an individual may easily exercise the rights

752 provided under this subsection.

753 (c) The OCABR shall establish and maintain on a website a searchable, publicly available,

754 central registry of third-party collecting entities that are registered with the OCABR under this

755 subsection that includes a listing of all registered data brokers and a search feature that allows

756 members of the public to identify individual data brokers and access to the registration

757 information provided under subsection (b).

758 (d) Penalties. A data broker that fails to register or provide the notice as required under

759 this section shall be liable for:—

760 (1) a civil penalty of \$100 for each day the data broker fails to register or provide notice

761 as required under this section, not to exceed a total of \$10,000 for any year; and

762 (2) an amount equal to the registration fees for each year that the data broker failed to

763 register as required under this subsection.

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

766 Section 11. Civil rights protections

767 (a) A covered entity or a service provider may not collect, process, or transfer covered  
768 data or publicly available data in a manner that discriminates in or otherwise makes unavailable  
769 the equal enjoyment of goods or services (i.e., has a disparate impact) on the basis of race, color,  
770 religion, national origin, sex, sexual orientation, gender identity or disability.

771 (b) This subsection shall not apply to:—

772 (1) the collection, processing, or transfer of covered data for the purpose of:—

773 (i) covered entity's or a service provider's self-testing to prevent or mitigate unlawful  
774 discrimination; or

775 (ii) diversifying an applicant, participant, or customer pool; or

776 (2) any private club or group not open to the public, as described in section 201(e) of the  
777 Civil Rights Act of 1964, 42 U.S.C. section 2000a(e).

778 (c) Whenever the Attorney General obtains information that a covered entity or service  
779 provider may have collected, processed, or transferred covered data in violation of subsection  
780 (a), the Attorney General shall initiate enforcement actions relating to such violation in  
781 accordance with section (14) this chapter.

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

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

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

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

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

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

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

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

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

805 (A)covered minors;

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

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

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

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

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

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

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

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

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

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

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

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

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

842 Section 12. Miscellaneous

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

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

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

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

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

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

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

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

858 (1)1 or more qualified employees as privacy officers; and

859 (2)1 or more qualified employees as data security officers.

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

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

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

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

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

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

874 (1)reasonable and appropriate in scope given:—

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

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

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

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

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

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

886 Section 13. Service providers.

887 (a)A service provider:—

888 (1)shall adhere to the instructions of a covered entity and only collect, process, and  
889 transfer service provider data to the extent necessary and proportionate to provide a service  
890 requested by the covered entity, as set out in the contract required by subsection (b), and this  
891 paragraph does not require a service provider to collect, process, or transfer covered data if the  
892 service provider would not otherwise do so;

893 (2)may not collect, process, or transfer service provider data if the service provider has  
894 actual knowledge that a covered entity violated this chapter with respect to such data;

895 (3)shall assist a covered entity in responding to a request made by an individual under  
896 this chapter, by either:—

897 (i)providing appropriate technical and organizational measures, considering the nature of  
898 the processing and the information reasonably available to the service provider, for the covered  
899 entity to comply with such request for service provider data; or

900 (ii)fulfilling a request by a covered entity to execute an individual rights request that the  
901 covered entity has determined should be complied with, by either:—

902 (A)complying with the request pursuant to the covered entity’s instructions; or

903 (B)providing written verification to the covered entity that it does not hold covered data  
904 related to the request, that complying with the request would be inconsistent with its legal  
905 obligations, or that the request falls within an exception under this chapter;

906 (4) may engage another service provider for purposes of processing service provider  
907 data on behalf of a covered entity only after providing that covered entity with notice and  
908 pursuant to a written contract that requires such other service provider to satisfy the obligations  
909 of the service provider with respect to such service provider data, including that the other service  
910 provider be treated as a service provider under this chapter;

911 (5)shall, upon the reasonable request of the covered entity, make available to the covered  
912 entity information necessary to demonstrate the compliance of the service provider with the  
913 requirements of this chapter, which may include making available a report of an independent  
914 assessment arranged by the service provider on terms agreed to by the service provider and the  
915 covered entity, providing information necessary to enable the covered entity to conduct and  
916 document a privacy impact assessment required by this chapter;

917 (6)shall, at the covered entity’s direction, delete or return all covered data to the covered  
918 entity as requested at the end of the provision of services, unless retention of the covered data is  
919 required by law;

920 (7) shall develop, implement, and maintain reasonable administrative, technical, and  
921 physical safeguards that are designed to protect the security and confidentiality of covered data  
922 the service provider processes consistent with chapter 93H of the general laws; and

923 (8) shall allow and cooperate with reasonable assessments by the covered entity or  
924 the covered entity's designated assessor. Alternatively, the service provider may arrange for a  
925 qualified and independent assessor to conduct an assessment of the service provider's policies  
926 and technical and organizational measures in support of the obligations under this chapter using  
927 an appropriate and accepted control standard or framework and assessment procedure for such  
928 assessments. The service provider shall provide a report of such assessment to the covered entity  
929 upon request.

930 (b) A person or entity may only act as a service provider pursuant to a written contract  
931 between the covered entity and the service provider, or a written contract between one service  
932 provider and a second service provider as described under paragraph (4) of subsection (a), if the  
933 contract:—

934 (1) sets forth the data processing procedures of the service provider with respect to  
935 collection, processing, or transfer performed on behalf of the covered entity or service provider;

936 (2) clearly sets forth:—

937 (i) instructions for collecting, processing, or transferring data;

938 (ii) the nature and purpose of collecting, processing, or transferring;

939 (iii) the type of data subject to collecting, processing, or transferring;

940 (iv) the duration of processing; and

941 (v)the rights and obligations of both parties, including a method by which the service  
942 provider shall notify the covered entity of material changes to its privacy practices;

943 (3)does not relieve a covered entity or a service provider of any requirement or liability  
944 imposed on such covered entity or service provider under this chapter; and

945 (4)prohibits:—

946 (i)collecting, processing, or transferring covered data in contravention to subsection (a);  
947 and

948 (ii)combining service provider data with covered data which the service provider receives  
949 from or on behalf of another person or persons or collects from the interaction of the service  
950 provider with an individual, provided that such combining is not necessary to effectuate a  
951 purpose described in paragraphs (1) through (15) of section 2(a) and is otherwise permitted under  
952 the contract required by this subsection.

953 (c)Each service provider shall retain copies of previous contracts entered into in  
954 compliance with this subsection with each covered entity to which it provides requested products  
955 or services.

956 (d)The classification of a person or entity as a covered entity or as a service provider and  
957 the relationship between covered entities and service providers are regulated by the following  
958 provisions:—

959 (1)Determining whether a person is acting as a covered entity or service provider with  
960 respect to a specific processing of covered data is a fact-based determination that depends upon  
961 the context in which such data is processed.

962 (2)A person or entity that is not limited in its processing of covered data pursuant to the  
963 instructions of a covered entity, or that fails to adhere to such instructions, is a covered entity and  
964 not a service provider with respect to a specific processing of covered data. A service provider  
965 that continues to adhere to the instructions of a covered entity with respect to a specific  
966 processing of covered data remains a service provider. If a service provider begins, alone or  
967 jointly with others, determining the purposes and means of the processing of covered data, it is a  
968 covered entity and not a service provider with respect to the processing of such data.

969 (3)A covered entity that transfers covered data to a service provider or a service provider  
970 that transfers covered data to a covered entity or another service provider, in compliance with the  
971 requirements of this chapter, is not liable for a violation of this chapter by the service provider or  
972 covered entity to whom such covered data was transferred, if at the time of transferring such  
973 covered data, the covered entity or service provider did not have actual knowledge that the  
974 service provider or covered entity would violate this chapter.

975 (4)A covered entity or service provider that receives covered data in compliance with the  
976 requirements of this chapter is not in violation of this chapter as a result of a violation by a  
977 covered entity or service provider from which such data was received.

978 (e)A third party:—

979 (1)shall not process third party data for a processing purpose other than the processing  
980 purpose for which—

981 (i)the individual gave affirmative express consent or to effect a purpose enumerated in  
982 paragraph (2), (3), or (5) of subsection (a) of section 2 in the case of sensitive covered data; or

983 (ii)the covered entity made a disclosure pursuant to their privacy policy and in the case of  
984 data that is not sensitive data;

985 (2)may reasonably rely on representations made by the covered entity that transferred the  
986 third-party data if the third party conducts reasonable due diligence on the representations of the  
987 covered entity and finds those representations to be credible.

988 (f)Solely for the purposes of this section, the requirements for service providers to  
989 contract with, assist, and follow the instructions of covered entities shall be read to include  
990 requirements to contract with, assist, and follow the instructions of a government entity if the  
991 service provider is providing a service to a government entity.

992 Section 14. Enforcement. Private Right of Action and Attorney General enforcement.

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

995 (b)Private right of action. Any individual alleging a violation of this chapter by a covered  
996 entity that is not a small business may bring a civil action in the superior court or any court of  
997 competent jurisdiction.

998 (c)An individual protected by this chapter may not be required, as a condition of service  
999 or otherwise, to file an administrative complaint with the commission or to accept mandatory  
1000 arbitration of a claim under this chapter.

1001 (d)The civil action shall be directed to the covered entity, data processor, and the third-  
1002 parties alleged to have committed the violation.

1003 (e)In a civil action in which the plaintiff prevails, the court may award:—

1004 (1)liquidated damages of not less than 0.15% of the annual global revenue of the covered  
1005 entity or \$15,000 per violation, whichever is greater;

1006 (2)punitive damages; and

1007 (3)any other relief, including but not limited to an injunction, that the court deems to be  
1008 appropriate.

1009 (f)In addition to any relief awarded pursuant to the previous paragraph, the court shall  
1010 award reasonable attorney’s fees and costs to any prevailing plaintiff.

1011 (g)The attorney general may bring an action pursuant to section 4 of chapter 93A against  
1012 a covered entity, service provider, third party or data broker to remedy violations of this chapter  
1013 and for other relief that may be appropriate.

1014 (1)If the court finds that the defendant has employed any method, chapter, or practice  
1015 which they knew or should have known to be in violation of this chapter, the court may require  
1016 such person to pay to the commonwealth a civil penalty of:—

1017 (i)not less than 0.15% of the annual global revenue or \$15,000, whichever is greater, per  
1018 violation; and

1019 (ii)not more than 4% of the annual global revenue of the covered entity, data processor,  
1020 or third-party or \$20,000,000, whichever is greater, per action if such action includes multiple  
1021 violations to multiple individuals;

1022 (2)All money awards shall be paid to the commonwealth. The commonwealth shall  
1023 identify the individuals affected by the violation and earmark such money awards, penalties, or

1024 assessments collected for purposes of paying for the damages they suffered as a consequence of  
1025 the violation.

1026 (h)When calculating awards and civil penalties in all the actions in this section, the court  
1027 shall consider:—

1028 (1)the number of affected individuals;

1029 (2)the severity of the violation or noncompliance;

1030 (3)the risks caused by the violation or noncompliance;

1031 (4)whether the violation or noncompliance was part of a pattern of noncompliance and  
1032 violations and not an isolated instance;

1033 (5)whether the violation or noncompliance was willful and not the result of error;

1034 (6)the precautions taken by the defendant to prevent a violation;

1035 (7)the number of administrative actions, lawsuits, settlements, and consent-decrees under  
1036 this chapter involving the defendant;

1037 (8)the number of administrative actions, lawsuits, settlements, and consent-decrees  
1038 involving the defendant in other states and at the federal level in issues involving information  
1039 privacy; and

1040 (9)the international record of the defendant when it comes to information privacy issues.

1041 (i)It is a violation of this chapter for a covered entity or anyone else acting on behalf of a  
1042 covered entity to retaliate against an individual who makes a good-faith complaint that there has  
1043 been a failure to comply with any part of this chapter.

1044 (1)An injured individual by a violation of the previous paragraph may bring a civil action  
1045 for monetary damages and injunctive relief in any court of competent jurisdiction.

#### 1046 Section 15. Enforcement - Miscellaneous

1047 (a)Any provision of a contract or agreement of any kind, including a covered entity's  
1048 terms of service or a privacy policy, including the short-form privacy notice required under  
1049 section 3 that purports to waive or limit in any way an individual's rights under this chapter,  
1050 including but not limited to any right to a remedy or means of enforcement shall be deemed  
1051 contrary to public policy and shall be void and unenforceable.

1052 (b)No covered entity that is a provider of an interactive computer service, as defined in  
1053 47 U.S.C. section 230, shall be treated as the publisher or speaker of any personal information  
1054 provided by another information content provider, as defined in 47 U.S.C. section 230 and  
1055 allowing posting of information by a user without other action by the interactive computer  
1056 service shall not be deemed processing of the personal information by the interactive computer  
1057 service.

1058 (c)No private or government action brought pursuant to this chapter shall preclude any  
1059 other action under this chapter.

#### 1060 Section 16. Transparency

1061 (a)Covered entities that receive any form of a legal request for disclosure of personal  
1062 information pursuant to this chapter shall:—

1063 (1)provide the Attorney General and the general public a bi-monthly report containing the  
1064 following aggregate information related to legal requests received by the covered entity, their  
1065 affiliated data processors, and any third parties they contracted with:—

1066 (i)The total number of legal requests, disaggregated by type of requests such as warrants,  
1067 court orders, and subpoenas;

1068 (ii)The number of legal requests that resulted in the covered entity disclosing personal  
1069 information;

1070 (iii)The number of legal requests that did not result in the covered entity disclosing  
1071 personal information, including the reasons why the information was not disclosed;

1072 (iv)The type of personal information sought in the legal requests received by the covered  
1073 entity;

1074 (v)The total number of legal requests seeking the disclosure of location or biometric  
1075 information;

1076 (vi)The number of legal requests that resulted in the covered entity disclosing location or  
1077 biometric information;

1078 (vii)The number of legal requests that did not result in the covered entity disclosing  
1079 location or biometric information, including the reasons for such no disclosure; and

1080 (viii)The nature of the proceedings from which the requests were ordered and whether it  
1081 was a government entity or a private person seeking the legal request;

1082 (b)take all reasonable measures and engage in all legal actions available to ensure that the  
1083 legal request is valid under applicable laws and statutes; and

1084 (c)require their affiliate data processors and third parties they contracted with to have  
1085 similar practices and standards.

## 1086 Section 17. Non-applicability

1087 (a)This chapter shall not apply to:—

1088 (1)personal information captured from a patient by a health care provider or health care  
1089 facility or biometric information collected, processed, used, or stored exclusively for medical  
1090 education or research, public health or epidemiological purposes, health care treatment,  
1091 insurance, payment, or operations under the federal Health Insurance Portability and  
1092 Accountability chapter of 1996, or to X-ray, roentgen process, computed tomography, MRI, PET  
1093 scan, mammography, or other image or film of the human anatomy used exclusively to diagnose,  
1094 prognose, or treat an illness or other medical condition or to further validate scientific testing or  
1095 screening;

1096 (2)individuals sharing their personal contact information such as email addresses with  
1097 other individuals in the workplace, or other social, political, or similar settings where the purpose  
1098 of the information is to facilitate communication among such individuals, provided that this  
1099 chapter shall cover any processing of such contact information beyond interpersonal  
1100 communication; or

1101 (3)covered entities’ publication of entity-based member or employee contact information  
1102 where such publication is intended to allow members of the public to contact such member or  
1103 employee in the ordinary course of the entity’s operations.

1104 Section 18. Relationship with other laws

1105 (a)Nothing in this chapter shall diminish any individual’s rights or obligations under the  
1106 Massachusetts Fair Information Practices chapter and its regulations.

1107 Section 19. Implementation

1108 (a)The Attorney General shall:—

1109 (1)adopt, amend, or repeal regulations for the implementation, administration, and  
1110 enforcement of this chapter;

1111 (2)gather facts and information applicable to the Attorney General’s obligation to enforce  
1112 this chapter and ensure its compliance;

1113 (3)conduct investigations for possible violations of this chapter;

1114 (4)refer cases for criminal prosecution to the appropriate federal, state, or local  
1115 authorities; and

1116 (5)maintain an official internet website outlining the provisions of this Act.

1117 Section 20. Severability

1118 (a)Should any provision of this chapter or part hereof be held under any circumstances in  
1119 any jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect  
1120 the validity or enforceability of any other provision of this or other parts of this chapter.

1121 SECTION 2. Chapter 149 of the General Laws, as appearing in the 2018 Official Edition,  
1122 is hereby amended by inserting after section 203 the following section:—

1123 Section 204. Workplace Surveillance

1124 (a)For the purposes of this section, the following words shall have the following  
1125 meanings unless the context clearly requires otherwise:—

1126 (1)"Information" also referred to as "employee information," or "employee data",  
1127 information that identifies, relates to, describes, is reasonably capable of being associated with,  
1128 or could reasonably be linked, directly or indirectly, with a particular employee, regardless of  
1129 how the information is collected, inferred, or obtained.

1130 (2)"Electronic monitoring", the collection of information concerning employee activities,  
1131 communications, actions, biometrics, or behaviors by electronic means.

1132 (3)"Employment-related decision", any decision made by the employer that affects  
1133 wages, benefits, hours, work schedule, performance evaluation, hiring, discipline, promotion,  
1134 termination, job content, productivity requirements, workplace health and safety, or any other  
1135 terms and conditions of employment.

1136 (4)"Vendor", a business engaged in a contract with an employer to provide services,  
1137 software, or technology that collects, stores, analyzes, or interprets employee information.

1138 (5)“Facial recognition technology” shall have the meaning established in section 220 of  
1139 chapter 6 of the General Laws, as amended by Chapter 253 of the Acts of 2020.

1140 (b)An employer, or vendor acting on behalf of an employer, shall not electronically  
1141 monitor an employee unless:—

1142 (1)the electronic monitoring only purpose is to:—

1143 (i)enable tasks that are necessary to accomplish essential job functions;

1144 (ii)monitor production processes or quality;

1145 (iii)comply with employment, labor, or other relevant laws;

1146 (iv)protect the safety and security of employees; or

1147 (v)carry on other purposes as determined by the department of labor standards; and

1148 (2)the specific form of electronic monitoring is:—

1149 (i)necessary to accomplish the allowable purpose;

1150 (ii)the least invasive means that could reasonably be used to accomplish the allowable  
1151 purpose;

1152 (iii)limited to the smallest number of employees; and

1153 (iv)collecting the least amount of information necessary to accomplish the purpose  
1154 mentioned in (1).

1155 (c)Notwithstanding subsection (b), the following practices shall be prohibited:—

1156 (1)use of electronic monitoring that either directly or indirectly harms an employee's  
1157 physical health, mental health, personal safety or wellbeing;

1158 (2)monitoring of employees who are off-duty and not performing work-related tasks;

1159 (3)audio-visual monitoring of bathrooms or other similarly private areas including locker  
1160 rooms and changing areas;

1161 (4)audio-visual monitoring of break rooms, lounges, and other social spaces, except to  
1162 investigate specific illegal activity;

1163 (5)use of facial recognition technology other than for the purpose of verifying the identity  
1164 of an employee for security purposes; and

1165 (6)any other forms of electronic monitoring such as may be prohibited by the department  
1166 of labor standards.

1167 (d)Employers shall not require employees to install applications on personal or mobile  
1168 devices that collect employee information or require employees to wear data-collecting devices,  
1169 including those that are incorporated into items of clothing or personal accessories, unless the  
1170 electronic monitoring is necessary to accomplish essential job functions and is narrowly limited  
1171 to only the activities and times necessary to accomplish essential job functions.

1172 (e)Information resulting from electronic monitoring shall be accessed only by authorized  
1173 agents and used only for the purpose and duration for which notice was given in accordance with  
1174 subsection (f).

1175 (f)Employers shall provide employees with notice that electronic monitoring will occur  
1176 prior to conducting each specific form of electronic monitoring. The notice must, at a minimum,  
1177 include:—

1178 (1)a description of:—

1179 (i)the purpose that the specific form of electronic monitoring is intended to accomplish,  
1180 as specified in subsection (b);

1181 (ii)the specific activities, locations, communications, and job roles that will be  
1182 electronically monitored;

1183 (iii)the technologies used to conduct the specific form of electronic monitoring;

1184 (iv)the vendors or other third parties that information collected through electronic  
1185 monitoring will be disclosed or transferred to, including the name of the vendor and the purpose  
1186 for the data transfer;

1187 (v)the organizational positions that are authorized to access the information collected  
1188 through the specific form of electronic monitoring, and under what conditions; and

1189 (vi)the dates, times, and frequency that electronic monitoring will occur;

1190 (2)the names of any vendors conducting electronic monitoring on the employer’s behalf;  
1191 and

1192 (3)an explanation of:—

1193 (i)the reasons why the specific form of electronic monitoring is necessary to accomplish  
1194 the purpose; and

1195 (ii)how the specific monitoring practice is the least invasive means available to  
1196 accomplish the allowable monitoring purpose.

1197 (g)The notice mentioned in (f) shall be clear and conspicuous and provide the employee  
1198 with actual notice of electronic monitoring activities.

1199 (1)A notice that provides electronic monitoring "may" take place or that the employer  
1200 "reserves the right" to monitor shall not suffice.

1201 (h)An employer who engages in random or periodic electronic monitoring of employees  
1202 will inform the affected employees of the specific events which are being monitored at the time  
1203 the monitoring takes place with a notice that shall be clear and conspicuous.

1204 (1)Notwithstanding the previous paragraph, notice of random or periodic electronic  
1205 monitoring may be given after electronic monitoring has occurred only if necessary to preserve  
1206 the integrity of an investigation of wrongdoing or protect the immediate safety of employees,  
1207 customers, or the public.

1208 (i)Employers shall provide a copy of the above notice disclosure to the department of  
1209 labor standards.

1210 (j)An employer shall only use employee information collected through electronic  
1211 monitoring to accomplish its purpose, unless the information documents illegal activity.

1212 (k)When making a hiring or employment-related decision using information collected  
1213 through electronic monitoring, an employer shall:—

1214 (1)not make the decision based solely on such information;

1215 (2)give the affected employee access to the data and provide an opportunity to correct or  
1216 explain it;

1217 (3)corroborate such information by other means, such as independent documentation by  
1218 supervisors or managers, or by consultation with other employees; and

1219 (4)document and communicate to affected employees the basis for the corroboration prior  
1220 to the decision going into effect.

1221 (l)Subsection (k) shall not apply to those cases when electronic monitoring data provides  
1222 evidence of illegal activity.

1223 SECTION 3. Effective date.

1224 (a)The provisions of this Act shall take effect 12 months after this Act is enacted.

1225 (b)The enforcement of chapter 93L shall be delayed until 6 months after the effective  
1226 date.