

**HOUSE . . . . . No.**

---

**The Commonwealth of Massachusetts**

PRESENTED BY:

*Andres X. Vargas and Simon Cataldo*

*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 to establish the Massachusetts neural data privacy protection act.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
<i>Andres X. Vargas</i>	<i>3rd Essex</i>	<i>1/17/2025</i>
<i>Simon Cataldo</i>	<i>14th Middlesex</i>	<i>1/17/2025</i>

**HOUSE . . . . . No.**

[Pin Slip]

**The Commonwealth of Massachusetts**

**In the One Hundred and Ninety-Fourth General Court  
(2025-2026)**

An Act to establish the Massachusetts neural 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.

2 The General Laws, as appearing in the 2022 Official Edition, are hereby amended by  
3 inserting after chapter 93L the following chapter:

4 Chapter 93N. Massachusetts Neural Data Privacy Protection Act

5 Section 1. Definitions

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

8 (1) “authentication”, the process of verifying an individual or entity for security  
9 purposes.

10 (2) "chapter”, this chapter of the General Laws, as from time to time may be  
11 amended, and any regulations promulgated under said chapter.

12           (3)     “collect” and “collection”, buying, renting, licensing, gathering, obtaining,  
13 receiving, accessing, or otherwise acquiring covered data by any means.

14           (4)     “consent”, a clear affirmative act signifying an individual’s freely given, specific,  
15 informed, and unambiguous agreement to allow the processing of specific categories of personal  
16 information relating to the individual for a narrowly defined particular purpose after having been  
17 informed, in response to a specific request from a covered entity that meets the requirements of  
18 this chapter; provided, however, that “consent” may include a written statement, including a  
19 statement written by electronic means, or any other unambiguous affirmative action; and  
20 provided further, that the following shall not constitute “consent”:

21           (i)     acceptance of a general or broad terms of use or similar document that contains  
22 descriptions of personal information processing along with other, unrelated information;

23           (ii)    hovering over, muting, pausing, or closing a given piece of content; or

24           (iii)   agreement obtained through dark patterns or a false, fictitious, fraudulent, or  
25 materially misleading statement or representation.

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

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

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

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

32           (6)     “covered data”, information, including derived data, inferences, and unique  
33 persistent identifiers that identifies or is linked or reasonably linkable, alone or in combination  
34 with other information, to an individual or a device that identifies or is linked or reasonably  
35 linkable to an individual. However, the term “covered data” does not include de-identified data  
36 or publicly available information.

37           (7)     “covered entity”, any entity or any person, other than an individual acting in a  
38 non-commercial context, that alone or jointly with others determines the purposes and means of  
39 collecting, processing, or transferring covered data.

40           The term “covered entity” does not include:

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

43           (8)     “covered high-impact social media company”, a covered entity that provides any  
44 internet-accessible platform where:

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

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

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

50           (9)     “dark pattern or deceptive design”, a user interface that is designed, modified, or  
51 manipulated with the purpose or substantial effect of obscuring, subverting, or impairing a

52 reasonable individual’s autonomy, decision-making, or choice, including, but not limited to, any  
53 practice the Federal Trade Commission refers to as a “dark pattern.”

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

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

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

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

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

65 (iii) contractually obligates any person or entity that receives the information from the  
66 covered entity or service provider:

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

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

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

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

76 (13) “homepage”, the introductory page of an internet website and any internet web  
77 page where personal information is collected; provided, however, that in the case of an online  
78 service, such as a mobile application, “homepage” shall include:

79 (i) the application’s platform page or download page;

80 (ii) a link within the application, such as from the application configuration, “About,”  
81 “Information,” or settings page; and

82 (iii) any other location that allows individuals to review the notices required by this  
83 chapter, including, but not limited to, before downloading the application.

84 (14) “individual”, a natural person who is a Massachusetts resident or is present in  
85 Massachusetts.

86 (15) “knowledge”,

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

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

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

94           (16)    “large data holder”, a covered entity or service provider that in the most recent  
95 calendar year:

96           (i)     had annual gross revenues of \$200,000,000 or more; and

97           (ii)    collected, processed, or transferred the covered data of more than 2,000,000  
98 individuals or devices that identify or are linked or reasonably linkable to one or more  
99 individuals, excluding covered data collected and processed solely for the purpose of initiating,  
100 rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested  
101 product or service; or the sensitive covered data of more than 200,000 individuals or devices that  
102 identify or are linked or reasonably linkable to one or more individuals.

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

108           (17)    “material”, with respect to an act, practice, or representation of a covered entity  
109 (including a representation made by the covered entity in a privacy policy or similar disclosure to

110 individuals) involving the collection, processing, or transfer of covered data, that such act,  
111 practice, or representation is likely to affect a reasonable individual’s decision or conduct  
112 regarding a product or service

113 (18) “minor”, an individual under the age of 18.

114 (19) “neural data”, means information that is generated by measuring the activity of an  
115 individual’s central or peripheral nervous system, and that is not inferred from non-neural  
116 information.

117 (20) “OCABR”, the Office of Consumer Affairs and Business Regulation.

118 (21) “precise geolocation information,” information derived from a device or from  
119 interactions between devices, with or without the knowledge of the user and regardless of the  
120 technological method used, that pertains to or directly or indirectly reveals the present or past  
121 geographical location of an individual or device within the Commonwealth of Massachusetts  
122 with sufficient precision to identify street-level location information within a range of 1,850 feet  
123 or less.

124 (22) “process”, any operation or set of operations performed on information or on sets  
125 of information, whether or not by automated means, including but not limited to the use, storage,  
126 analysis, deletion, or modification of information.

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



131           (24) “profiling”, any form of automated processing performed on personal data to  
132 evaluate, analyze or predict personal aspects related to an identified or identifiable individual’s  
133 economic situation, health, personal preferences, interests, reliability, behavior, location or  
134 movements.

135           (25) “publicly available information”, any information that a covered entity or service  
136 provider has a reasonable basis to believe has been lawfully made available to the general public  
137 from:

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

141           (ii) widely distributed media;

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

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

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

149           For purposes of this paragraph, information from a website or online service is not  
150 available to all members of the public if the individual who made the information available via  
151 the website or online service has either restricted the information to a specific audience or

152 reasonably expects that the information will not be distributed to so many persons as to become a  
153 matter of public knowledge.

154 The term “publicly available information” does not include neural data.

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

158 (27) “sensitive covered data”, a form of covered data, including neural data.

159 (i) neural data;

160 (ii) covered data processed from neural data concerning an individual’s past, present  
161 or future mental or physical health condition, disability, diagnosis or treatment, including  
162 pregnancy and cosmetic treatment;

163 (28) “service provider”, a person or entity that:

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

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

168 A service provider that receives service provider data from another service provider as  
169 permitted under this chapter shall be treated as a service provider under this chapter with respect  
170 to such data.

171 (29) “service provider data”, covered data that is collected or processed by or has been  
172 transferred to a service provider by or on behalf of a covered entity or a government agency or  
173 another service provider for the purpose of allowing the service provider to whom such covered  
174 data is transferred to perform a service or function on behalf of, and at the direction of, such  
175 covered entity or government agency.

176 (30) “targeted advertising”, presenting to an individual or device identified by a unique  
177 identifier, or groups of individuals or devices identified by unique identifiers, an online  
178 advertisement that is selected based on known or predicted preferences, characteristics, or  
179 interests associated with the individual or a device identified by a unique identifier; provided,  
180 however, that “targeted advertising” does not include:

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

183 (ii) contextual advertising, which is when an advertisement is displayed based on the  
184 content with or in which the advertisement appears and does not vary based on who is viewing  
185 the advertisement; or

186 (iii) processing covered data strictly necessary for the sole purpose of measuring or  
187 reporting advertising or content performance, reach, or frequency, including independent  
188 measurement.

189 (31) “third party”, any person or entity, including a covered entity, that

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

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

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

197 (32) "third party data", covered data that has been transferred to a third party.

198 (33) "transfer", to disclose, sell, release, disseminate, make available, license, rent, or  
199 share covered data orally, in writing, electronically, or by any other means.

200 (34) "unique identifier", an identifier to the extent that such identifier is reasonably  
201 linkable to an individual or device that identifies or is linked or reasonably linkable to 1 or more  
202 individuals, including a device identifier, Internet Protocol address, cookie, beacon, pixel tag,  
203 mobile ad identifier, or similar technology, customer number, unique pseudonym, user alias,  
204 telephone number, or other form of persistent or probabilistic identifier that is linked or  
205 reasonably linkable to an individual or device. This term does not include an identifier assigned  
206 by a covered entity for the specific purpose of giving effect to an individual's exercise of consent  
207 or opt-outs of the collection, processing, and transfer of covered data pursuant to this chapter or  
208 otherwise limiting the collection, processing, or transfer of such information.

209 (35) "widely distributed media", information that is available to the general public,  
210 including information from a telephone book or online directory, a television, internet, or radio

211 program, the news media, or an internet site that is available to the general public on an  
212 unrestricted basis, but does not include an obscene visual depiction, as defined in 18 U.S.C.  
213 section 1460.

## 214 Section 2. Sensitive Covered Data

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

216 (1) collect or process sensitive covered data, except where such collection or  
217 processing is strictly necessary to provide or maintain a specific product or service requested by  
218 the individual to whom the covered data pertains.

219 (2) transfer an individual's sensitive covered data to a third party, unless:

220 (i) the transfer is made pursuant to the consent of the individual, given before each  
221 specific transfer takes place;

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

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

228 (3) process sensitive covered data for the purposes of targeted advertising.

## 229 Section 3. Data Subject Rights

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

232           (1)     access:

233           (i)     in a human-readable format that a reasonable individual can understand and  
234 download from the internet and transmit freely, the covered data (except covered data in a back-  
235 up or archival system) of the individual making the request that is collected, processed, or  
236 transferred by the covered entity or any service provider of the covered entity within the 12  
237 months preceding the request;

238           (ii)    the categories of any third party or service provider, if applicable, and an option  
239 for consumers to obtain the names of any such third party as well as and the categories of any  
240 service providers to whom the covered entity has transferred the covered data of the individual,  
241 as well as the categories of sources from which the covered data was collected; and

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

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

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

255 (i) a human-readable format that a reasonable individual can understand and  
256 download from the internet and transmit freely; and

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

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

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

262 (2) the use of any dark pattern or deceptive design.

263 (c) Subject to subsections (d) and (e), each request under subsection (a) shall be  
264 completed within 45 days of such request from an individual, unless it is demonstrably  
265 impracticable or impracticably costly to verify such individual's request.

266 (d) A response period set forth in this subsection may be extended once by 20  
267 additional days when reasonably necessary, considering the complexity and number of the  
268 individual's requests, so long as the covered entity informs the individual of any such extension  
269 within the initial 45-day response period, together with the reason for the extension.

270 (e) A covered entity:

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

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

275 (ii) any time beyond the initial two times described in subparagraph (i), may allow the  
276 individual to exercise such right for a reasonable fee for each request.

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

279 (1) cannot reasonably verify that the individual making the request to exercise the  
280 right is the individual whose covered data is the subject of the request or an agent authorized to  
281 make such a request on the individual's behalf;

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

284 (3) determines that the exercise of the right would require access to or correction of  
285 another individual's sensitive covered data;

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

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



290 (g) If a covered entity cannot reasonably verify that a request to exercise a right  
291 described in subsection (a) is made by the individual whose covered data is the subject of the  
292 request, the covered entity:

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

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

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

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

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

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

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

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

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

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

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

319 (9) prevent a covered entity from being able to maintain a confidential record of  
320 deletion requests, maintained solely for the purpose of preventing covered data of an individual  
321 from being recollected after the individual submitted a deletion request and requested that the  
322 covered entity no longer collect, process, or transfer such data; or

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

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

327 (1) unreasonably interferes with the provision of products or services by the covered  
328 entity to another person it currently serves;

329 (2) requests to delete covered data reasonably necessary to perform a contract  
330 between the covered entity and the individual;

331 (3) requests to delete covered data that the covered entity needs to retain in order to  
332 comply with professional ethical obligations;

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

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

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

340 (l) A covered entity shall facilitate the ability of individuals to make requests under  
341 subsection (a) in any language in which the covered entity provides a product or service. The  
342 mechanisms by which a covered entity enables individuals to make requests under subsection (a)  
343 shall be readily accessible and usable by individuals with disabilities. Such mechanisms shall, at  
344 a minimum, be accessible in the same or a similar location as the privacy policies required by  
345 section 9 of this chapter.

#### 346 Section 4. Consent Practices

347 (a) The requirements of this chapter with respect to a request for consent from a  
348 covered entity or service provider to an individual are the following:

349 (1) The request for consent shall be provided to the individual in a clear and  
350 conspicuous standalone disclosure made through the primary medium used to offer the covered  
351 entity's product or service, or, in the case that the product or service is not offered in a medium

352 that does permit the making of the request under this paragraph, another medium regularly used  
353 in conjunction with the covered entity's product or service;

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

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

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

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

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

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

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

370 (7) Processing or transferring any covered data collected pursuant to consent for a  
371 different processing purpose than that for which consent was obtained shall require consent for  
372 the subsequent processing purpose;

373 (8) The request for consent must be displayed at or before the point of collection; and

374 (9) The request must be accompanied by a copy of the covered entity's or service  
375 provider's privacy policy subject to the requirements of section 9, which may be included with  
376 the request as a hyperlink, and, if the covered entity is a large data holder, shall also include the  
377 short form privacy policy as required by subsection (h) of section 9.

378 (b) A covered entity shall not infer that an individual has provided consent to a  
379 practice from the inaction of the individual or the individual's continued use of a service or  
380 product provided by the covered entity.

381 (c) A covered entity shall not obtain or attempt to obtain the consent of an individual  
382 through:

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

385 (2) the use of any dark pattern or deceptive design; or

386 (3) conditioning or limiting access to an individual's account.

#### 387 Section 5. Privacy by Design

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

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

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

394 (3) mitigate privacy risks related to the products and services of the covered entity or  
395 the service provider, including in the design, development, and implementation of such products  
396 and services, considering the role of the covered entity or service provider and the information  
397 available to it;

398 (4) evaluate the length of time that covered data shall be retained and circumstances  
399 under which covered data shall be deleted, de-identified, or otherwise modified with respect to  
400 the purposes for which it was collected or processed and the sensitivity of the covered data; and

401 (5) implement reasonable training and safeguards within the covered entity and  
402 service provider to promote compliance with all privacy laws applicable to covered data the  
403 covered entity collects, processes, or transfers or covered data the service provider collects,  
404 processes, or transfers on behalf of the covered entity and mitigate privacy risks taking into  
405 account the role of the covered entity or service provider and the information available to it.

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

408 (1) the size of the covered entity or the service provider and the nature, scope, and  
409 complexity of the activities engaged in by the covered entity or service provider, including  
410 whether the covered entity or service provider is a large data holder, nonprofit organization,  
411 small business, or third party, considering the role of the covered entity or service provider and  
412 the information available to it;

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

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

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

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

#### 421 Section 6. Pricing

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

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

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

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

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

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

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

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

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

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

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

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

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



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

456 Section 7. Civil Rights Protections

457 (a) A covered entity or a service provider may not collect, process, or transfer  
458 covered data or publicly available data in a manner that discriminates in or otherwise makes  
459 unavailable the equal enjoyment of goods or services (i.e., has a disparate impact) on the basis of  
460 race, color, religion, national origin, sex, sexual orientation, gender identity, disability, genetic  
461 information, neural data, pregnancy or a condition related to said pregnancy including, but not  
462 limited to, lactation or the need to express breast milk for a nursing child, ancestry or status as a  
463 veteran, or any other basis protected by chapter 151B.

464 (b) This subsection shall not apply to:

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

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

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

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

471 (c) Whenever the Attorney General obtains information that a covered entity or  
472 service provider may have collected, processed, or transferred covered data in violation of  
473 subsection (a), the Attorney General shall initiate enforcement actions relating to such violation  
474 in accordance with section 12 of this chapter.

475                   (1)     Not later than 3 years after the date of enactment of this chapter, and  
476 annually no later than December 31 of each year thereafter, the Attorney General shall submit to  
477 the joint committee on ways and means, the joint committee on racial equity, civil rights, and  
478 inclusion, and the joint committee on advanced information technology, the internet and  
479 cybersecurity a report that includes a summary of the enforcement actions taken under this  
480 subsection.

481                   Section 8. Privacy Policy

482                   (a)     Each covered entity or service provider shall make publicly available, in a clear  
483 and conspicuous location on its homepage, a reasonably understandable and not misleading  
484 privacy policy that provides a detailed and accurate representation of the data collection,  
485 processing, and transfer activities of the covered entity or service provider.

486                   (b)     The privacy policy must be provided in a manner that is reasonably accessible to  
487 and usable by individuals with disabilities. The policy shall be made available to the public in  
488 each covered language in which the covered entity or service provider provides a product or  
489 service that is subject to the privacy policy; or carries out activities related to such product or  
490 service.

491                   (c)     The privacy policy must include, at a minimum:

492                   (1)     The identity and the contact information of:

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

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

498 (2) the categories of covered data the covered entity or service provider collects or  
499 processes;

500 (3) the processing purposes for each category of covered data the covered entity or  
501 service provider collects or processes;

502 (4) whether the covered entity or service provider transfers covered data and, if so,  
503 each category of service provider and third party to which the covered entity or service provider  
504 transfers covered data, and the purposes for which such data is transferred to such categories of  
505 service providers and third parties or third-party collecting entities, except for a transfer to a  
506 governmental entity pursuant to a court order or law that prohibits the covered entity or service  
507 provider from disclosing such transfer;

508 (5) The length of time the covered entity or service provider intends to retain each  
509 category of covered data, including sensitive covered data, or, if it is not possible to identify that  
510 timeframe, the criteria used to determine the length of time the covered entity or service provider  
511 intends to retain categories of covered data;

512 (6) A prominent, clear, and reasonably understandable description of how an  
513 individual can exercise the rights described in this chapter;

514 (7) A general description of the covered entity's or service provider's data security  
515 practices; and

516 (8) The effective date of the privacy policy.

517           (d)     If a covered entity or service provider makes a material change to its privacy  
518 policy or practices, the covered entity or service provider shall notify each individual affected by  
519 such material change before implementing the material change with respect to any prospectively  
520 collected covered data and provide a reasonable opportunity for each individual to withdraw  
521 consent to any further materially different collection, processing, or transfer of previously  
522 collected covered data under the changed policy.

523           (e)     A covered entity or service provider shall take all reasonable electronic measures  
524 to provide direct notification regarding material changes to the privacy policy to each affected  
525 individual, in each covered language in which the privacy policy is made available, and taking  
526 into account available technology and the nature of the relationship.

527           (f)     Nothing in this section shall be construed to affect the requirements for covered  
528 entities or service providers under other sections of this chapter.

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

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

540 (i) Each covered entity or service provider that collects, processes, or transfers  
541 biometric data shall provide a separate privacy policy detailing the collection, processing, and  
542 transfer of such biometric data, subject to the provisions of subsections (a) through (h) of this  
543 section.

544 (j) Each covered entity or service provider that collects, processes, or transfers  
545 specific precise geolocation information shall provide a separate privacy policy detailing the  
546 collection, processing, and transfer of such precise geolocation information, subject to the  
547 provisions of subsections (a) through (h) of this section.

#### 548 Section 9. Advanced Data Rights

549 (a) A covered entity or service provider shall provide an individual with a clear and  
550 conspicuous, easy-to-execute means to withdraw consent. Those means shall be at least as easy  
551 to execute by an individual as the means to provide consent and shall, at a minimum, be  
552 accessible in the same or a substantially similar location as the privacy policies required by  
553 section 8.

554 (b) A covered entity or service provider shall provide an individual with a clear and  
555 conspicuous, easy-to-execute means to opt out of covered data transfers. Those means shall be at  
556 least as easy to execute by an individual as the means to provide consent and shall, at a  
557 minimum, be accessible in the same or a substantially similar location as the privacy policies  
558 required by section 8.

559 (c) Right to opt out of profiling. A covered entity or service provider that engages in  
560 profiling in furtherance of automated decisions that produce legal or similarly significant effects  
561 on an individual shall:

562 (1) provide such individual with a clear and conspicuous means to opt out of such  
563 profiling; and

564 (2) allow an individual to object to such profiling through an opt out mechanism, at a  
565 minimum, accessible in the same or a substantially similar location as the privacy policies  
566 required by section 9.

567 (d) A covered entity or service provider that receives an opt out notification pursuant  
568 to this section shall abide by such opt out designations in a commercially reasonable timeframe.  
569 Such covered entity or service provider shall notify any other person that directed the covered  
570 entity or service provider to either serve, deliver, or otherwise process targeted advertisements or  
571 to engage in profiling in furtherance of automated decisions of the individual's opt out decision  
572 within a commercially reasonable timeframe.

573 (e) A covered entity or service provider may not condition, effectively condition,  
574 attempt to condition, or attempt to effectively condition the exercise of any individual right under  
575 this section through:

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

578 (2) the use of a dark pattern or deceptive design.

579 (f) A covered entity shall notify third parties who had access to an individual's  
580 covered data when the individual exercises any of the rights established in this section. The third  
581 party shall comply with the request to opt out of sale or data transfer forwarded to them from a  
582 covered entity that provided, made available, or authorized the collection of the individual's  
583 covered data. The third party shall comply with the request in the same way a covered entity is  
584 required to comply with the request. The third party shall no longer retain, use, or disclose the  
585 personal information unless the third party becomes a service provider or a covered entity in the  
586 terms of this chapter.

587 (g) A covered entity that communicates an individual's opt out request to a third  
588 party or service provider pursuant to this section shall not be liable under this chapter if the third  
589 party or service provider receiving the opt-out request violates the restrictions set forth in this  
590 chapter; provided, however, that at the time of communicating the opt-out request, the covered  
591 entity does not know or should not reasonably know that the third party or service provider  
592 intends to commit such a violation.

593 (h) If an individual decides to opt out of the processing of the individual's covered  
594 data for the purposes specified in subsections (b), (c), or (d) and such decision conflicts with the  
595 individual's existing, voluntary participation in a covered entity's bona fide loyalty, rewards,  
596 premium features, discounts or club card program, the covered entity shall comply with the  
597 individual's opt out preference signal but may notify the individual of the conflict and provide  
598 the individual with the choice to opt back into such processing for participation in such a  
599 program; provided, however, that the controller shall not use dark patterns or deceptive design to  
600 coerce the individual to opt back into such processing related to that individual's participation in  
601 such program.

602 (i) A covered entity or service provider shall not require an individual to create an  
603 account for the purposes of exercising any right under this chapter.

604 Section 10. Service Providers

605 (a) A service provider:

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

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

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

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

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

620 (A) complying with the request pursuant to the covered entity's instructions; or



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

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

629 (5) shall, upon the reasonable request of the covered entity, make available to the  
630 covered entity information necessary to demonstrate the compliance of the service provider with  
631 the requirements of this chapter, which may include making available a report of an independent  
632 assessment arranged by the service provider on terms agreed to by the service provider and the  
633 covered entity or providing information necessary to enable the covered entity to conduct and  
634 document a privacy impact assessment;

635 (6) shall, at the covered entity's direction, delete or return all covered data to the  
636 covered entity as requested at the end of the provision of services, unless retention of the covered  
637 data is required by law;

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

641 (8) shall allow and cooperate with reasonable assessments by the covered entity or  
642 the covered entity's designated assessor. Alternatively, the service provider may arrange for a

643 qualified and independent assessor to conduct an assessment of the service provider's policies  
644 and technical and organizational measures in support of the obligations under this chapter using  
645 an appropriate and accepted control standard or framework and assessment procedure for such  
646 assessments. The service provider shall provide a report of such assessment to the covered entity  
647 upon request.

648 (b) A person or entity may only act as a service provider pursuant to a written  
649 contract between the covered entity and the service provider, or a written contract between one  
650 service provider and a second service provider as described under paragraph (4) of subsection  
651 (a), if the contract:

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

654 (2) clearly sets forth:

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

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

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

658 (iv) the duration of processing; and

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

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

663 (4) prohibits:

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

666 (ii) combining service provider data with covered data which the service provider  
667 receives from or on behalf of another person or persons or collects from the interaction of the  
668 service provider with an individual, provided that such combining is otherwise permitted under  
669 the contract required by this subsection.

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

673 (d) The classification of a person or entity as a covered entity or as a service provider  
674 and the relationship between covered entities and service providers are regulated by the  
675 following provisions:

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

679 (2) A person or entity that is not limited in its processing of covered data pursuant to  
680 the instructions of a covered entity, or that fails to adhere to such instructions, is a covered entity  
681 and not a service provider with respect to a specific processing of covered data. A service  
682 provider that continues to adhere to the instructions of a covered entity with respect to a specific  
683 processing of covered data remains a service provider. If a service provider begins, alone or

684 jointly with others, determining the purposes and means of the processing of covered data, it is a  
685 covered entity and not a service provider with respect to the processing of such data.

686 (3) A covered entity that transfers covered data to a service provider or a service  
687 provider that transfers covered data to a covered entity or another service provider, in  
688 compliance with the requirements of this chapter, is not liable for a violation of this chapter by  
689 the service provider or covered entity to whom such covered data was transferred, if at the time  
690 of transferring such covered data, the covered entity or service provider did not have actual  
691 knowledge that the service provider or covered entity would violate this chapter.

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

695 (e) A third party:

696 (1) shall not process third party data for a processing purpose other than the  
697 processing purpose for which

698 (i) the individual gave consent or to effect a purpose enumerated in paragraph (1),  
699 (2), or (3) of subsection (a) of section 2 in the case of sensitive covered data; or

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

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

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

709 Section 11. Enforcement

710 (a) A violation of this chapter constitutes an injury to that individual and shall be  
711 deemed an unfair or deceptive act or practice in the conduct of trade or commerce under chapter  
712 93A, provided that if the court finds for any petitioner, subject to section 9, paragraph (3) of such  
713 chapter, recovery under such chapter shall be in the amount of actual damages or \$5,000,  
714 whichever is higher.

715 (b) Private right of action. Any individual alleging a violation of this chapter by a  
716 covered entity, service provider, or third party that is a large data holder may bring a civil action  
717 in the superior court or any court of competent jurisdiction.

718 (c) An individual protected by this chapter may not be required, as a condition of  
719 service or otherwise, to file an administrative complaint with the attorney general or to accept  
720 mandatory arbitration of a claim under this chapter.

721 (d) The civil action shall be directed to the covered entity, service provider, and third-  
722 parties alleged to have committed the violation.

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

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

726 (2) punitive damages; and

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

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

731 (g) The Attorney General may bring an action pursuant to section 4 of chapter 93A  
732 against a covered entity, service provider, or third party to remedy violations of this chapter and  
733 for other relief, including but not limited to an injunction, that may be appropriate, subject to the  
734 following:

735 (1) If the court finds that the defendant has employed any method, act, or practice  
736 which they knew or should have known to be in violation of this chapter, the court may require  
737 the defendant to pay to the commonwealth a civil penalty of:

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

740 (ii) not more than 4% of the annual global revenue of the covered entity, service  
741 provider, or third-party or \$20,000,000, whichever is greater, per action if such action includes  
742 multiple violations to multiple individuals;

743 (2) If the court finds that a defendant has engaged in flagrant, willful and repeat  
744 violations of this chapter, the court may issue an order to suspend or prohibit a covered entity,  
745 service provider, or third party from operating in the commonwealth or collecting, processing,

746 and transferring covered data and any other relief, including but not limited to an injunction, that  
747 the court deems to be appropriate.

748 (3) In addition to any penalty or relief awarded under this subsection, a defendant  
749 violating this chapter shall also be liable to the commonwealth for the reasonable costs of  
750 investigation and litigation of such violation, including reasonable attorneys' fees and reasonable  
751 expert fees.

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

754 (1) the number of affected individuals;

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

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

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

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

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

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

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

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

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

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

773 (j) Any provision of a contract or agreement of any kind, including a covered entity's  
774 terms of service or a privacy policy, including the short-form privacy notice required under  
775 section 8 subsection (h) that purports to waive or limit in any way an individual's rights under  
776 this chapter, including but not limited to any right to a remedy or means of enforcement shall be  
777 deemed contrary to public policy and shall be void and unenforceable.

778 (k) No private or government action brought pursuant to this chapter shall preclude  
779 any other action under this chapter.

## 780 Section 12. Information Non-applicability

781 (a) This chapter shall not apply to only the following specific types of information:

782 (1) personal information captured from a patient by a health care provider or health  
783 care facility or biometric information collected, processed, used, or stored exclusively for  
784 medical education or research, public health or epidemiological purposes, health care treatment,  
785 insurance, payment, or operations under the federal Health Insurance Portability and  
786 Accountability Act of 1996, or to X-ray, roentgen process, computed tomography, MRI, PET



787 scan, mammography, or other image or film of the human anatomy used exclusively to diagnose,  
788 prognose, or treat an illness or other medical condition or to further validate scientific testing or  
789 screening;

790 (2) nonpublic personal information that is processed by a financial institution subject  
791 to, and in compliance with, the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq., as amended  
792 from time to time;

793 (3) personal information regulated by the federal Family Educational Rights and  
794 Privacy Act, 20 U.S.C. 1232g et seq., as amended from time to time;

795 (4) individuals sharing their personal contact information such as email addresses  
796 with other individuals in the workplace, or other social, political, or similar settings where the  
797 purpose of the information is to facilitate communication among such individuals, provided that  
798 this chapter shall cover any processing of such contact information beyond interpersonal  
799 communication; or

800 (5) covered entities' publication of entity-based member or employee contact  
801 information where such publication is intended to allow members of the public to contact such  
802 member or employee in the ordinary course of the entity's operations.

803 (b) For the purpose of this section, the burden of proving that information is exempt  
804 from the provisions of this chapter shall be upon the party claiming the exemption.

805 Section 13. Implementation

806 (a) The Attorney General shall adopt rules and regulations for the implementation,  
807 administration, and enforcement of this chapter and may from time to time amend or repeal said  
808 regulations. The rules and regulations shall include but are not limited to:

809 (1) establishing or adopting baseline technical requirements that determine if a given  
810 dataset has been or can be considered sufficiently de-identified;

811 (2) establishing reasonable policies, practices, and procedures that satisfy the  
812 requirements set forward in Section 5;

813 (3) establishing a nonexclusive list of practices that constitute deceptive designs or  
814 dark patterns or otherwise violate the requirements set forward in Section 4.

815 (b) The Attorney General may:

816 (1) gather facts and information applicable to the Attorney General's obligation to  
817 enforce this chapter and ensure its compliance, consistent with the provisions of section 4 of  
818 chapter 93A;

819 (2) conduct investigations for possible violations of this chapter; and

820 (3) refer cases for civil enforcement or criminal prosecution to the appropriate  
821 federal, state, or local authorities.

822 (c) The Attorney General shall, within one year after the effective date of chapter,  
823 create an official internet website that outlines the provisions of this chapter and provides  
824 individuals with a form or other mechanism to report violations of this chapter to the Office of  
825 the Attorney General. The Attorney General shall update the website at least annually. The

826 website shall include statistics on the Attorney General’s enforcement actions undertaken under  
827 this chapter, broken down by fiscal year, including but not limited to:

- 828 (1) number of complaints received;
- 829 (2) number of open investigations;
- 830 (3) number of closed investigations; and
- 831 (4) a summary of case dispositions in which a violation of this chapter occurred.

832 Section 14. Authorized Agents

833 (a) An individual may designate another person to serve as the individual’s  
834 authorized agent to exercise the individual’s rights under section 3, to withdraw consent under  
835 section 9, or opt out of the processing of such individual's covered data for one or more of the  
836 purposes specified in section 9.

837 (b) An individual may designate an authorized agent as provided in subsection (a) by  
838 technological means, including, but not limited to, an Internet link or a browser setting, browser  
839 extension or global device setting that indicates the individual’s intent to opt out processing for  
840 one or more of the purposes specified in section 9.

841 (c) A covered entity or service provider shall comply with a request received from an  
842 authorized agent if the covered entity or service provider is able to verify the identity of the  
843 individual and the authorized agent's authority to act on such individual’s behalf by the same  
844 means and subject to the same restrictions as a covered entity under section 3(g).

845 (d) In the case of covered data concerning an individual known to be a child as  
846 defined by the Children’s Online Privacy Protection Act, 15 U.S.C. 6501, the parent or legal  
847 guardian of such child may exercise the rights provided under this chapter on the child's behalf.

848 (e) In the case of covered data concerning an individual subject to a guardianship,  
849 conservatorship or other protective arrangement, the guardian or the conservator of the  
850 individual may exercise the rights provided under this chapter on the individual's behalf.

#### 851 Section 15. Severability and Relationship to Other Laws

852 (a) Should any provision of this chapter or part hereof be held under any  
853 circumstances in any court of competent jurisdiction to be invalid or unenforceable, such  
854 invalidity or unenforceability shall not affect the validity or enforceability of any other provision  
855 of this or other parts of this chapter.

856 (b) Nothing in this chapter shall diminish any individual’s rights or obligations under  
857 chapters 66A, 93A, 93H, or under sections 1B or 3B of chapter 214.

#### 858 SECTION 2. Effective Date

859 This Act shall take effect 1 year after enactment.