

HOUSE No. 97

The Commonwealth of Massachusetts

PRESENTED BY:

David M. Rogers and Andres X. Vargas

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

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

An Act protecting consumers in interactions with artificial intelligence systems.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
<i>David M. Rogers</i>	<i>24th Middlesex</i>	<i>1/17/2025</i>
<i>Andres X. Vargas</i>	<i>3rd Essex</i>	<i>1/17/2025</i>
<i>Patrick Joseph Kearney</i>	<i>4th Plymouth</i>	<i>5/20/2025</i>

HOUSE No. 97

By Representatives Rogers of Cambridge and Vargas of Haverhill, a petition (accompanied by bill, House, No. 97) of David M. Rogers and Andres X. Vargas relative to consumers interactions with artificial intelligence systems. Advanced Information Technology, the Internet and Cybersecurity.

The Commonwealth of Massachusetts

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

An Act protecting consumers in interactions with artificial intelligence systems.

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 2022 Official Edition, are hereby
2 amended by inserting a new chapter:

3 CHAPTER 93M. Consumer Protections in interactions with Artificial Intelligence
4 Systems

5 Section 1. Definitions

6 The following words shall, unless the context clearly requires otherwise, have the
7 following meanings:—

8 "Algorithmic discrimination" means any condition in which the use of an artificial
9 intelligence system results in an unlawful differential treatment or impact that disfavors an
10 individual or group of individuals on the basis of their actual or perceived age, color, disability,
11 ethnicity, genetic information, limited proficiency in the English language, national origin, race,

12 religion, reproductive health, sex, veteran status, or other classification protected under the laws
13 of this state or federal law.

14 "Algorithmic discrimination" does not include:

15 (1) the offer, license, or use of a high-risk artificial intelligence system by a developer or
16 deployer for the sole purpose of:

17 (i) the developer's or deployer's self-testing to identify, mitigate, or prevent
18 discrimination or otherwise ensure compliance with state and federal law; or

19 (ii) expanding an applicant, customer, or participant pool to increase diversity or redress
20 historical discrimination; or

21 (2) an act or omission by or on behalf of a private club or other establishment that is not
22 in fact open to the public, as set forth in Title II of the federal "Civil Rights Act of 1964", 42
23 U.S.C. Sec. 2000a (e), as amended.

24 "Artificial intelligence system" means any machine-based system that, for any explicit or
25 implicit objective, infers from the inputs the system receives how to generate outputs, including
26 content, decisions, predictions, or recommendations, that can influence physical or virtual
27 environments.

28 "Consequential decision" means a decision that has a material legal or similarly
29 significant effect on the provision or denial to any consumer of, or the cost or terms of:

30 (1) education enrollment or an education opportunity;

31 (2) employment or an employment opportunity;

- 32 (3) a financial or lending service;
- 33 (4) an essential government service;
- 34 (5) health-care services;
- 35 (6) housing;
- 36 (7) insurance; or
- 37 (8) a legal service.

38 "Consumer" means an individual who is a Massachusetts resident.

39 "Deploy" means to use a high-risk artificial intelligence system.

40 "Deployer" means a person doing business in this state that deploys a high-risk artificial
41 intelligence system.

42 "Developer" means a person doing business in this state that develops or intentionally
43 and substantially modifies an artificial intelligence system.

44 "Health-care services" has the same meaning as provided in 42 U.S.C. Sec. 234 (d)(2).

45 "High-risk artificial intelligence system" means any artificial intelligence system that,
46 when deployed, makes, or is a substantial factor in making, a consequential decision.

47 "High-risk artificial intelligence system" does not include:

- 48 (1) an artificial intelligence system if the artificial intelligence system is intended to:
- 49 (i) perform a narrow procedural task; or

50 (ii) detect decision-making patterns or deviations from prior decision-making patterns
51 and is not intended to replace or influence a previously completed human assessment without
52 sufficient human review; or

53 (2) the following technologies, unless the technologies, when deployed, make, or are a
54 substantial factor in making, a consequential decision:

55 (i) anti-fraud technology that does not use facial recognition technology;

56 (ii) anti-malware;

57 (iii) anti-virus;

58 (iv) artificial intelligence-enabled video games;

59 (v) calculators;

60 (vi) cybersecurity;

61 (vii) databases;

62 (viii) data storage;

63 (ix) firewall;

64 (x) internet domain registration;

65 (xi) internet website loading;

66 (xii) networking;

67 (xiii) spam- and robocall-filtering;

68 (xiv) spell-checking;

69 (xv) spreadsheets;

70 (xvi) web caching;

71 (xvii) web hosting or any similar technology; or

72 (xviii) technology that communicates with consumers in natural language for the purpose
73 of providing users with information, making referrals or recommendations, and answering
74 questions and is subject to an accepted use policy that prohibits generating content that is
75 discriminatory or harmful.

76 "Intentional and substantial modification" or "intentionally and substantially modifies"
77 means a deliberate change made to an artificial intelligence system that results in any new
78 reasonably foreseeable risk of algorithmic discrimination.

79 "Intentional and substantial modification" or "intentionally and substantially modifies"
80 does not include a change made to a high-risk artificial intelligence system, or the performance
81 of a high-risk artificial intelligence system, if:

82 (1) the high-risk artificial intelligence system continues to learn after the high-risk
83 artificial intelligence system is:

84 (i) offered, sold, leased, licensed, given, or otherwise made available to a deployer; or

85 (ii) deployed;

86 (2) the change is made to the high-risk artificial intelligence system as a result of any
87 learning described in paragraph (1)(i) of this subsection;

88 (3) the change was predetermined by the deployer, or a third party contracted by the
89 deployer, when the deployer or third party completed an initial impact assessment of such high-
90 risk artificial intelligence system pursuant to section 3 (c) (1); and

91 (4) the change is included in technical documentation for the high-risk artificial
92 intelligence system.

93 "Substantial factor" means a factor that:

94 (1) assists in making a consequential decision;

95 (2) is capable of altering the outcome of a consequential decision; and

96 (3) is generated by an artificial intelligence system.

97 "Substantial factor" includes any use of an artificial intelligence system to generate any
98 content, decision, prediction, or recommendation concerning a consumer that is used as a basis to
99 make a consequential decision concerning the consumer.

100 "Trade secret" has the meaning set forth in section 42 (4) of chapter 93 of the General
101 Laws, as appearing in the 2022 Official Edition.

102 Section 2. Developer duty to avoid algorithmic discrimination - required documentation.

103 (a) Not later than 6 months after the effective date of this act, a developer of a high-risk
104 artificial intelligence system shall use reasonable care to protect consumers from any known or
105 reasonably foreseeable risks of algorithmic discrimination arising from the intended and
106 contracted uses of the high-risk artificial intelligence system. In any enforcement action brought
107 not later than 6 months after the effective date of this act, by the attorney general pursuant to

108 section 6, there is a rebuttable presumption that a developer used reasonable care as required
109 under this section if the developer complied with this section and any additional requirements or
110 obligations as set forth in rules promulgated by the attorney general pursuant to section 7.

111 (b) Not later than 6 months after the effective date of this act, and except as provided in
112 subsection (f) of this section, a developer of a high-risk artificial intelligence system shall make
113 available to the deployer or other developer of the high-risk artificial intelligence system:

114 (1) a general statement describing the reasonably foreseeable uses and known harmful or
115 inappropriate uses of the high-risk artificial intelligence system;

116 (2) documentation disclosing:

117 (i) high-level summaries of the type of data used to train the high-risk artificial
118 intelligence system;

119 (ii) known or reasonably foreseeable limitations of the high-risk artificial intelligence
120 system, including known or reasonably foreseeable risks of algorithmic discrimination arising
121 from the intended uses of the high-risk artificial intelligence system;

122 (iii) the purpose of the high-risk artificial intelligence system;

123 (iv) the intended benefits and uses of the high-risk artificial intelligence system; and

124 (v) all other information necessary to allow the deployer to comply with the requirements
125 of section 3;

126 (3) documentation describing:

127 (i) how the high-risk artificial intelligence system was evaluated for performance and
128 mitigation of algorithmic discrimination before the high-risk artificial intelligence system was
129 offered, sold, leased, licensed, given, or otherwise made available to the deployer;

130 (ii) the data governance measures used to cover the training datasets and the measures
131 used to examine the suitability of data sources, possible biases, and appropriate mitigation;

132 (iii) the intended outputs of the high-risk artificial intelligence system;

133 (iv) the measures the developer has taken to mitigate known or reasonably foreseeable
134 risks of algorithmic discrimination that may arise from the reasonably foreseeable deployment of
135 the high-risk artificial intelligence system; and

136 (v) how the high-risk artificial intelligence system should be used, not be used, and be
137 monitored by an individual when the high-risk artificial intelligence system is used to make, or is
138 a substantial factor in making, a consequential decision; and

139 (4) any additional documentation that is reasonably necessary to assist the deployer in
140 understanding the outputs and monitor the performance of the high-risk artificial intelligence
141 system for risks of algorithmic discrimination.

142 (c) (1) except as provided in subsection (f) of this section, a developer that offers, sells,
143 leases, licenses, gives, or otherwise makes available to a deployer or other developer a high-risk
144 artificial intelligence system not later than 6 months after the effective date of this act, shall
145 make available to the deployer or other developer, to the extent feasible, the documentation and
146 information, through artifacts such as model cards, dataset cards, or other impact assessments,

147 necessary for a deployer, or for a third party contracted by a deployer, to complete an impact
148 assessment pursuant to section 3 (c).

149 (2) a developer that also serves as a deployer for a high-risk artificial intelligence system
150 is not required to generate the documentation required by this section unless the high-risk
151 artificial intelligence system is provided to an unaffiliated entity acting as a deployer.

152 (d) (1) Not later than 6 months after the effective date of this act, a developer shall make
153 available, in a manner that is clear and readily available on the developer's website or in a public
154 use case inventory, a statement summarizing:

155 (i) the types of high-risk artificial intelligence systems that the developer has developed
156 or intentionally and substantially modified and currently makes available to a deployer or other
157 developer; and

158 (ii) how the developer manages known or reasonably foreseeable risks of algorithmic
159 discrimination that may arise from the development or intentional and substantial modification of
160 the types of high-risk artificial intelligence systems described in accordance with subsection
161 (d)(1)(i) of this section.

162 (2) a developer shall update the statement described in subsection (d)(1) of this section:

163 (i) as necessary to ensure that the statement remains accurate; and

164 (ii) no later than ninety days after the developer intentionally and substantially modifies
165 any high-risk artificial intelligence system described in subsection (d)(1)(i) of this section.

166 (e) Not later than 6 months after the effective date of this act, a developer of a high-risk
167 artificial intelligence system shall disclose to the attorney general, in a form and manner

168 prescribed by the attorney general, and to all known deployers or other developers of the high-
169 risk artificial intelligence system, any known or reasonably foreseeable risks of algorithmic
170 discrimination arising from the intended uses of the high-risk artificial intelligence system
171 without unreasonable delay but no later than ninety days after the date on which:

172 (1) the developer discovers through the developer's ongoing testing and analysis that the
173 developer's high-risk artificial intelligence system has been deployed and has caused or is
174 reasonably likely to have caused algorithmic discrimination; or

175 (2) the developer receives from a deployer a credible report that the high-risk artificial
176 intelligence system has been deployed and has caused algorithmic discrimination.

177 (f) nothing in subsections (b) to (e) of this section requires a developer to disclose a trade
178 secret, information protected from disclosure by state or federal law, or information that would
179 create a security risk to the developer.

180 (g) Not later than 6 months after the effective date of this act, the attorney general may
181 require that a developer disclose to the attorney general, no later than ninety days after the
182 request and in a form and manner prescribed by the attorney general, the statement or
183 documentation described in subsection (b) of this section. The attorney general may evaluate
184 such statement or documentation to ensure compliance with this chapter, and the statement or
185 documentation is not subject to disclosure under the "Massachusetts Public Records Law",
186 chapter 66, section 10 of the General Laws. In a disclosure pursuant to this subsection (g), a
187 developer may designate the statement or documentation as including proprietary information or
188 a trade secret. To the extent that any information contained in the statement or documentation

189 includes information subject to attorney-client privilege or work-product protection, the
190 disclosure does not constitute a waiver of the privilege or protection.

191 Section 3. Deployer duty to avoid algorithmic discrimination - risk management policy
192 and program.

193 (a) Not later than 6 months after the effective date of this act, a deployer of a high-risk
194 artificial intelligence system shall use reasonable care to protect consumers from any known or
195 reasonably foreseeable risks of algorithmic discrimination. In any enforcement action brought
196 not later than 6 months after the effective date of this act, by the attorney general pursuant to
197 section 6, there is a rebuttable presumption that a deployer of a high-risk artificial intelligence
198 system used reasonable care as required under this section if the deployer complied with this
199 section and any additional requirements or obligations as set forth in rules promulgated by the
200 attorney general pursuant to section 7.

201 (b) (1) Not later than 6 months after the effective date of this act, and except as provided
202 in subsection (f) of this section, a deployer of a high-risk artificial intelligence system shall
203 implement a risk management policy and program to govern the deployer's deployment of the
204 high-risk artificial intelligence system. The risk management policy and program must specify
205 and incorporate the principles, processes, and personnel that the deployer uses to identify,
206 document, and mitigate known or reasonably foreseeable risks of algorithmic discrimination.
207 The risk management policy and program must be an iterative process planned, implemented,
208 and regularly and systematically reviewed and updated over the life cycle of a high-risk artificial
209 intelligence system, requiring regular, systematic review and updates. A risk management policy

210 and program implemented and maintained pursuant to this subsection (b) must be reasonable
211 considering:

212 (i) (A) the guidance and standards set forth in the latest version of the "Artificial
213 Intelligence Risk Management Framework" published by the National Institute of Standards and
214 Technology in the United States Department of Commerce, standard ISO/IEC 42001 of the
215 International Organization for Standardization, or another nationally or internationally
216 recognized risk management framework for artificial intelligence systems, if the standards are
217 substantially equivalent to or more stringent than the requirements of this chapter; or

218 (B) any risk management framework for artificial intelligence systems that the attorney
219 general, in the attorney general's discretion, may designate;

220 (ii) the size and complexity of the deployer;

221 (iii) the nature and scope of the high-risk artificial intelligence systems deployed by the
222 deployer, including the intended uses of the high-risk artificial intelligence systems; and

223 (iv) the sensitivity and volume of data processed in connection with the high-risk
224 artificial intelligence systems deployed by the deployer.

225 (2) a risk management policy and program implemented pursuant to subsection (b)(1) of
226 this section may cover multiple high-risk artificial intelligence systems deployed by the
227 deployer.

228 (c) (1) except as provided in subsections (c)(4), (c)(5), and (f) of this section:

229 (i) a deployer, or a third party contracted by the deployer, that deploys a high-risk
230 artificial intelligence system not later than 6 months after the effective date of this act, shall
231 complete an impact assessment for the high-risk artificial intelligence system; and

232 (ii) Not later than 6 months after the effective date of this act, a deployer, or a third party
233 contracted by the deployer, shall complete an impact assessment for a deployed high-risk
234 artificial intelligence system at least annually and within ninety days after any intentional and
235 substantial modification to the high-risk artificial intelligence system is made available.

236 (2) an impact assessment completed pursuant to this subsection (c) must include, at a
237 minimum, and to the extent reasonably known by or available to the deployer:

238 (i) a statement by the deployer disclosing the purpose, intended use cases, and
239 deployment context of, and benefits afforded by, the high-risk artificial intelligence system;

240 (ii) an analysis of whether the deployment of the high-risk artificial intelligence system
241 poses any known or reasonably foreseeable risks of algorithmic discrimination and, if so, the
242 nature of the algorithmic discrimination and the steps that have been taken to mitigate the risks;

243 (iii) a description of the categories of data the high-risk artificial intelligence system
244 processes as inputs and the outputs the high-risk artificial intelligence system produces;

245 (iv) if the deployer used data to customize the high-risk artificial intelligence system, an
246 overview of the categories of data the deployer used to customize the high-risk artificial
247 intelligence system;

248 (v) any metrics used to evaluate the performance and known limitations of the high-risk
249 artificial intelligence system;

250 (vi) a description of any transparency measures taken concerning the high-risk artificial
251 intelligence system, including any measures taken to disclose to a consumer that the high-risk
252 artificial intelligence system is in use when the high-risk artificial intelligence system is in use;
253 and

254 (vii) a description of the post-deployment monitoring and user safeguards provided
255 concerning the high-risk artificial intelligence system, including the oversight, use, and learning
256 process established by the deployer to address issues arising from the deployment of the high-
257 risk artificial intelligence system.

258 (3) in addition to the information required under subsection (3)(b) of this section, an
259 impact assessment completed pursuant to this subsection (c) following an intentional and
260 substantial modification to a high-risk artificial intelligence system not later than 6 months after
261 the effective date of this act, must include a statement disclosing the extent to which the high-
262 risk artificial intelligence system was used in a manner that was consistent with, or varied from,
263 the developer's intended uses of the high-risk artificial intelligence system.

264 (4) a single impact assessment may address a comparable set of high-risk artificial
265 intelligence systems deployed by a deployer.

266 (5) if a deployer, or a third party contracted by the deployer, completes an impact
267 assessment for the purpose of complying with another applicable law or regulation, the impact
268 assessment satisfies the requirements established in this subsection (c) if the impact assessment
269 is reasonably similar in scope and effect to the impact assessment that would otherwise be
270 completed pursuant to this subsection (c).

271 (6) a deployer shall maintain the most recently completed impact assessment for a high-
272 risk artificial intelligence system as required under this subsection (c), all records concerning
273 each impact assessment, and all prior impact assessments, if any, for at least three years
274 following the final deployment of the high-risk artificial intelligence system.

275 (7) Not later than 6 months after the effective date of this act, and at least annually
276 thereafter, a deployer, or a third party contracted by the deployer, must review the deployment of
277 each high-risk artificial intelligence system deployed by the deployer to ensure that the high-risk
278 artificial intelligence system is not causing algorithmic discrimination.

279 (d) (1) Not later than 6 months after the effective date of this act, and no later than the
280 time that a deployer deploys a high-risk artificial intelligence system to make, or be a substantial
281 factor in making, a consequential decision concerning a consumer, the deployer shall:

282 (i) notify the consumer that the deployer has deployed a high-risk artificial intelligence
283 system to make, or be a substantial factor in making, a consequential decision before the decision
284 is made;

285 (ii) provide to the consumer a statement disclosing the purpose of the high-risk artificial
286 intelligence system and the nature of the consequential decision; the contact information for the
287 deployer; a description, in plain language, of the high-risk artificial intelligence system; and
288 instructions on how to access the statement required by subsection (5)(a) of this section; and

289 (iii) provide to the consumer information, if applicable, regarding the consumer's right to
290 opt out of the processing of personal data concerning the consumer for purposes of profiling in
291 furtherance of decisions that produce legal or similarly significant effects concerning the
292 consumer.

293 (2) Not later than 6 months after the effective date of this act, a deployer that has
294 deployed a high-risk artificial intelligence system to make, or be a substantial factor in making, a
295 consequential decision concerning a consumer shall, if the consequential decision is adverse to
296 the consumer, provide to the consumer:

297 (i) a statement disclosing the principal reason or reasons for the consequential decision,
298 including:

299 (A) the degree to which, and manner in which, the high-risk artificial intelligence system
300 contributed to the consequential decision;

301 (B) the type of data that was processed by the high-risk artificial intelligence system in
302 making the consequential decision; and

303 (C) the source or sources of the data described in subsection (d)(2)(i)(B) of this section;

304 (ii) an opportunity to correct any incorrect personal data that the high-risk artificial
305 intelligence system processed in making, or as a substantial factor in making, the consequential
306 decision; and

307 (iii) an opportunity to appeal an adverse consequential decision concerning the consumer
308 arising from the deployment of a high-risk artificial intelligence system, which appeal must, if
309 technically feasible, allow for human review unless providing the opportunity for appeal is not in
310 the best interest of the consumer, including in instances in which any delay might pose a risk to
311 the life or safety of such consumer.

312 (3) (i) except as provided in subsection (d)(3)(ii) of this section, a deployer shall provide
313 the notice, statement, contact information, and description required by subsections (c)(1) and
314 (d)(2) of this section:

315 (A) directly to the consumer;

316 (B) in plain language;

317 (C) in all languages in which the deployer, in the ordinary course of the deployer's
318 business, provides contracts, disclaimers, sale announcements, and other information to
319 consumers; and

320 (D) in a format that is accessible to consumers with disabilities.

321 (ii) if the deployer is unable to provide the notice, statement, contact information, and
322 description required by subsections (d)(1) and (d)(2) of this section directly to the consumer, the
323 deployer shall make the notice, statement, contact information, and description available in a
324 manner that is reasonably calculated to ensure that the consumer receives the notice, statement,
325 contact information, and description.

326 (e) (1) Not later than 6 months after the effective date of this act, and except as provided
327 in subsection (f) of this section, a deployer shall make available, in a manner that is clear and
328 readily available on the deployer's website, a statement summarizing:

329 (i) the types of high-risk artificial intelligence systems that are currently deployed by the
330 deployer;

331 (ii) how the deployer manages known or reasonably foreseeable risks of algorithmic
332 discrimination that may arise from the deployment of each high-risk artificial intelligence system
333 described pursuant to subsection (e)(1)(i) of this section; and

334 (iii) in detail, the nature, source, and extent of the information collected and used by the
335 deployer.

336 (2) a deployer shall periodically update the statement described in subsection (e)(1) of
337 this section.

338 (f) subsections (b), (c), and (e) of this section do not apply to a deployer if, at the time the
339 deployer deploys a high-risk artificial intelligence system and at all times while the high-risk
340 artificial intelligence system is deployed:

341 (1) the deployer:

342 (i) employs fewer than fifty full-time equivalent employees; and

343 (ii) does not use the deployer's own data to train the high-risk artificial intelligence
344 system;

345 (2) the high-risk artificial intelligence system:

346 (i) is used for the intended uses that are disclosed to the deployer as required by section 2
347 (b)(1); and

348 (ii) continues learning based on data derived from sources other than the deployer's own
349 data; and

350 (3) the deployer makes available to consumers any impact assessment that:

351 (i) the developer of the high-risk artificial intelligence system has completed and
352 provided to the deployer; and

353 (ii) includes information that is substantially similar to the information in the impact
354 assessment required under of this section.

355 (g) if a deployer deploys a high-risk artificial intelligence system not later than 6 months
356 after the effective date of this act, and subsequently discovers that the high-risk artificial
357 intelligence system has caused algorithmic discrimination, the deployer, without unreasonable
358 delay, but no later than ninety days after the date of the discovery, shall send subsection (c)(2) to
359 the attorney general, in a form and manner prescribed by the attorney general, a notice disclosing
360 the discovery.

361 (h) nothing in subsections (b) to (e) and (g) of this section requires a deployer to disclose
362 a trade secret or information protected from disclosure by state or federal law. To the extent that
363 a deployer withholds information pursuant to this subsection (h) or section 5 (e), the deployer
364 shall notify the consumer and provide a basis for the withholding.

365 (i) Not later than 6 months after the effective date of this act, the attorney general may
366 require that a deployer, or a third party contracted by the deployer, disclose to the attorney
367 general, no later than ninety days after the request and in a form and manner prescribed by the
368 attorney general, the risk management policy implemented pursuant to subsection (b) of this
369 section, the impact assessment completed pursuant to subsection (c) of this section, or the
370 records maintained pursuant to subsection (c)(6) of this section. The attorney general may
371 evaluate the risk management policy, impact assessment, or records to ensure compliance with
372 this chapter, and the risk management policy, impact assessment, and records are not subject to

373 disclosure under the “Massachusetts Public Records Law”, chapter 66, section 10 of the General
374 Laws. In a disclosure pursuant to this subsection (i), a deployer may designate the statement or
375 documentation as including proprietary information or a trade secret. To the extent that any
376 information contained in the risk management policy, impact assessment, or records include
377 information subject to attorney-client privilege or work-product protection, the disclosure does
378 not constitute a waiver of the privilege or protection.

379 Section 4. Disclosure of an artificial intelligence system to consumer

380 (a) Not later than 6 months after the effective date of this act, and except as provided in
381 subsection (b) of this section, a deployer or other developer that deploys, offers, sells, leases,
382 licenses, gives, or otherwise makes available an artificial intelligence system that is intended to
383 interact with consumers shall ensure the disclosure to each consumer who interacts with the
384 artificial intelligence system that the consumer is interacting with an artificial intelligence
385 system.

386 (b) disclosure is not required under subsection (a) of this section under circumstances in
387 which it would be obvious to a reasonable person that the person is interacting with an artificial
388 intelligence system.

389 Section 5. Compliance with other legal obligations - definitions

390 (a) nothing in this chapter restricts a developer's, a deployer's, or other person's ability to:

391 (1) comply with federal, state, or municipal laws, ordinances, or regulations;

392 (2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or
393 summons by a federal, a state, a municipal, or other governmental authority;

394 (3) cooperate with a law enforcement agency concerning conduct or activity that the
395 developer, deployer, or other person reasonably and in good faith believes may violate federal,
396 state, or municipal laws, ordinances, or regulations;

397 (4) investigate, establish, exercise, prepare for, or defend legal claims;

398 (5) take immediate steps to protect an interest that is essential for the life or physical
399 safety of a consumer or another individual;

400 (6) by any means other than the use of facial recognition technology, prevent, detect,
401 protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or
402 deceptive activities, or illegal activity; investigate, report, or prosecute the persons responsible
403 for any such action; or preserve the integrity or security of systems;

404 (7) engage in public or peer-reviewed scientific or statistical research in the public
405 interest that adheres to all other applicable ethics and privacy laws and is conducted in
406 accordance with 45 CFR 46, as amended, or relevant requirements established by the federal
407 Food and Drug Administration;

408 (8) conduct research, testing, and development activities regarding an artificial
409 intelligence system or model, other than testing conducted under real-world conditions, before
410 the artificial intelligence system or model is placed on the market, deployed, or put into service,
411 as applicable; or

412 (i) assist another developer, deployer, or other person with any of the obligations imposed
413 under this chapter.

414 (b) the obligations imposed on developers, deployers, or other persons under this chapter
415 do not restrict a developer's, a deployer's, or other person's ability to:

416 (1) effectuate a product recall; or

417 (2) identify and repair technical errors that impair existing or intended functionality.

418 (c) the obligations imposed on developers, deployers, or other persons under this chapter
419 do not apply where compliance with this chapter by the developer, deployer, or other person
420 would violate an evidentiary privilege under the laws of this state.

421 (d) nothing in this chapter imposes any obligation on a developer, a deployer, or other
422 person that adversely affects the rights or freedoms of a person, including the rights of a person
423 to freedom of speech or freedom of the press that are guaranteed in:

424 (1) the First Amendment to the United States constitution; or

425 (2) Part the First, Article XVI of the state constitution.

426 (e) nothing in this chapter applies to a developer, a deployer, or other person:

427 (1) insofar as the developer, deployer, or other person develops, deploys, puts into
428 service, or intentionally and substantially modifies, as applicable, a high-risk artificial
429 intelligence system:

430 (i) that has been approved, authorized, certified, cleared, developed, or granted by a
431 federal agency, such as the federal food and drug administration or the federal aviation
432 administration, acting within the scope of the federal agency's authority, or by a regulated entity
433 subject to the supervision and regulation of the federal housing finance agency; or

434 (ii) in compliance with standards established by a federal agency, including standards
435 established by the federal office of the national coordinator for health information technology, or
436 by a regulated entity subject to the supervision and regulation of the federal housing finance
437 agency, if the standards are substantially equivalent or more stringent than the requirements of
438 this chapter;

439 (2) conducting research to support an application for approval or certification from a
440 federal agency, including the federal Aviation Administration, the federal Communications
441 Commission, or the federal Food and Drug Administration or research to support an application
442 otherwise subject to review by the federal agency;

443 (3) performing work under, or in connection with, a contract with the United States
444 Department of Commerce, the United States Department of Defense, or the National Aeronautics
445 and Space Administration, unless the developer, deployer, or other person is performing the
446 work on a high-risk artificial intelligence system that is used to make, or is a substantial factor in
447 making, a decision concerning employment or housing; or

448 (4) that is a covered entity within the meaning of the federal "Health Insurance Portability
449 and Accountability Act of 1996", 42 U.S.C. Secs. 1320d to 1320d-9, and the regulations
450 promulgated under the federal act, as both may be amended from time to time, and is providing
451 health-care recommendations that:

452 (i) are generated by an artificial intelligence system;

453 (ii) require a health-care provider to take action to implement the recommendations; and

454 (iii) are not considered to be high risk.

455 (f) nothing in this chapter applies to any artificial intelligence system that is acquired by
456 or for the federal government or any federal agency or department, including the United States
457 Department of Commerce, the United States Department of Defense, or the National Aeronautics
458 and Space Administration, unless the artificial intelligence system is a high-risk artificial
459 intelligence system that is used to make, or is a substantial factor in making, a decision
460 concerning employment or housing.

461 (g) an insurer, as defined in chapter 175, a fraternal benefit society, as defined in chapter
462 176, or a developer of an artificial intelligence system used by an insurer is in full compliance
463 with this chapter if the insurer, the fraternal benefit society, or the developer is subject to the
464 requirements of chapter 175 and any rules adopted by the commissioner of insurance.

465 (h) (1) a bank, out-of-state bank, credit union chartered by the state of Massachusetts,
466 federal credit union, out-of-state credit union, or any affiliate or subsidiary thereof, is in full
467 compliance with this chapter if the bank, out-of-state bank, credit union chartered by the state of
468 Massachusetts, federal credit union, out-of-state credit union, or affiliate or subsidiary is subject
469 to examination by a state or federal prudential regulator under any published guidance or
470 regulations that apply to the use of high-risk artificial intelligence systems and the guidance or
471 regulations:

472 (i) impose requirements that are substantially equivalent to or more stringent than the
473 requirements imposed in this chapter; and

474 (ii) at a minimum, require the bank, out-of-state bank, credit union chartered by the state
475 of Massachusetts, federal credit union, out-of-state credit union, or affiliate or subsidiary to:

476 (A) regularly audit the bank's, out-of-state bank's, credit union chartered by the state of
477 Massachusetts', federal credit union's, out-of-state credit union's, or affiliate's or subsidiary's use
478 of high-risk artificial intelligence systems for compliance with state and federal anti-
479 discrimination laws and regulations applicable to the bank, out-of-state bank, credit union
480 chartered by the state of Massachusetts federal credit union, out-of-state credit union, or affiliate
481 or subsidiary; and

482 (B) mitigate any algorithmic discrimination caused by the use of a high-risk artificial
483 intelligence system or any risk of algorithmic discrimination that is reasonably foreseeable as a
484 result of the use of a high-risk artificial intelligence system.

485 (2) as used in this subsection (8):

486 (i) "Affiliate" has the meaning set forth in chapter 156D.

487 (ii) "Bank" has the meaning set forth in chapter 167.

488 (iii) "Credit union" has the meaning set forth in chapter 167.

489 (iv) "Out-of-state bank" has the meaning set forth in chapter 167.

490 (i) if a developer, a deployer, or other person engages in an action pursuant to an
491 exemption set forth in this section, the developer, deployer, or other person bears the burden of
492 demonstrating that the action qualifies for the exemption.

493 Section 6. Enforcement by attorney general

494 (a) the attorney general has exclusive authority to enforce this chapter.

495 (b) except as provided in subsection (c) of this section, a violation of the requirements
496 established in this chapter constitutes an unfair trade practice pursuant to chapter 93A.

497 (c) in any action commenced by the attorney general to enforce this chapter, it is an
498 affirmative that the developer, deployer, or other person:

499 (1) discovers and cures a violation of this this chapter 93 as a result of:

500 (i) feedback that the developer, deployer, or other person encourages deployers or users
501 to provide to the developer, deployer, or other person;

502 (ii) adversarial testing or red teaming, as those terms are defined or used by the national
503 institute of standards and technology; or

504 (iii) an internal review process; and

505 (2) is otherwise in compliance with:

506 (i) the latest version of the "Artificial intelligence risk management framework"
507 published by the national institute of standards and technology in the United States Department
508 of Commerce and Standard ISO/IEC 42001 of the International Organization for
509 Standardization;

510 (ii) another nationally or internationally recognized risk management framework for
511 artificial intelligence systems, if the standards are substantially equivalent to or more stringent
512 than the requirements of this chapter; or

513 (iii) any risk management framework for artificial intelligence systems that the attorney
514 general, in the attorney general's discretion, may designate and, if designated, shall publicly
515 disseminate.

516 (d) a developer, a deployer, or other person bears the burden of demonstrating to the
517 attorney general that the requirements established in subsection (3) of this section have been
518 satisfied.

519 (e) nothing in this chapter, including the enforcement authority granted to the attorney
520 general under this section, preempts or otherwise affects any right, claim, remedy, presumption,
521 or defense available at law or in equity. A rebuttable presumption or affirmative defense
522 established under this chapter applies only to an enforcement action brought by the attorney
523 general pursuant to this section and does not apply to any right, claim, remedy, presumption, or
524 defense available at law or in equity.

525 (f) this chapter does not provide the basis for, and is not subject to, a private right of
526 action for violations of this chapter or any other law.

527 Section 7. Rules

528 (a) the attorney general may promulgate rules as necessary for the purpose of
529 implementing and enforcing this chapter, including:

530 (1) the documentation and requirements for developers pursuant to section 2 (b);

531 (2) the contents of and requirements for the notices and disclosures required by sections 2

532 (c) and (g); 3 (d), (e), (g), and (i); and 4;

533 (3) the content and requirements of the risk management policy and program required by
534 section 3 (b);

535 (4) the content and requirements of the impact assessments required by section 3 (c);

536 (5) the requirements for the rebuttable presumptions set forth in sections 2 and 3; and

537 (6) the requirements for the affirmative defense set forth in section 6 (c), including the
538 process by which the attorney general will recognize any other nationally or internationally
539 recognized risk management framework for artificial intelligence systems.

540 SECTION 2: This law shall take effect no later than 6 months after the passage of this
541 bill.