



General Assembly

Amendment

January Session, 2023

LCO No. 7796



Offered by:

| | |
|---|--|
| SEN. MARONEY, 14 th Dist. | SEN. KUSHNER, 24 th Dist. |
| SEN. WINFIELD, 10 th Dist. | SEN. GASTON, 23 rd Dist. |
| REP. D'AGOSTINO, 91 st Dist. | SEN. MCCRORY, 2 nd Dist. |
| SEN. LOONEY, 11 th Dist. | SEN. RAHMAN, 4 th Dist. |
| SEN. DUFF, 25 th Dist. | SEN. LESSER, 9 th Dist. |
| SEN. HWANG, 28 th Dist. | SEN. LOPES, 6 th Dist. |
| SEN. KISSEL, 7 th Dist. | SEN. SLAP, 5 th Dist. |
| SEN. CICARELLA, 34 th Dist. | SEN. MAHER, 26 th Dist. |
| SEN. COHEN, 12 th Dist. | REP. MCCARTHY VAHEY, 133 rd Dist. |
| SEN. NEEDLEMAN, 33 rd Dist. | REP. KEITT, 134 th Dist. |
| SEN. OSTEN, 19 th Dist. | REP. CARPINO, 32 nd Dist. |
| SEN. CABRERA, 17 th Dist. | SEN. ANWAR, 3 rd Dist. |
| SEN. HOCHADEL, 13 th Dist. | SEN. MOORE, 22 nd Dist. |
| SEN. MARX, 20 th Dist. | |

To: Subst. Senate Bill No. 3

File No. 604

Cal. No. 347

"AN ACT CONCERNING ONLINE PRIVACY, DATA AND SAFETY PROTECTIONS."

1 Strike everything after the enacting clause and substitute the
2 following in lieu thereof:

3 "Section 1. Section 42-515 of the general statutes is repealed and the
4 following is substituted in lieu thereof (*Effective July 1, 2023*):

5 As used in this section and sections 42-516 to 42-525, inclusive, as
6 amended by this act, and section 2 of this act, unless the context

7 otherwise requires:

8 (1) "Abortion" means terminating a pregnancy for any purpose other
9 than producing a live birth.

10 [(1)] (2) "Affiliate" means a legal entity that shares common branding
11 with another legal entity or controls, is controlled by or is under
12 common control with another legal entity. For the purposes of this
13 subdivision, "control" [or] and "controlled" [means] mean (A)
14 ownership of, or the power to vote, more than fifty per cent of the
15 outstanding shares of any class of voting security of a company, (B)
16 control in any manner over the election of a majority of the directors or
17 of individuals exercising similar functions, or (C) the power to exercise
18 controlling influence over the management of a company.

19 [(2)] (3) "Authenticate" means to use reasonable means to determine
20 that a request to exercise any of the rights afforded under subdivisions
21 (1) to (4), inclusive, of subsection (a) of section 42-518 is being made by,
22 or on behalf of, the consumer who is entitled to exercise such consumer
23 rights with respect to the personal data at issue.

24 [(3)] (4) "Biometric data" means data generated by automatic
25 measurements of an individual's biological characteristics, such as a
26 fingerprint, a voiceprint, eye retinas, irises or other unique biological
27 patterns or characteristics that are used to identify a specific individual.
28 "Biometric data" does not include (A) a digital or physical photograph,
29 (B) an audio or video recording, or (C) any data generated from a digital
30 or physical photograph, or an audio or video recording, unless such
31 data is generated to identify a specific individual.

32 [(4)] (5) "Business associate" has the same meaning as provided in
33 HIPAA.

34 [(5)] (6) "Child" has the same meaning as provided in COPPA.

35 [(6)] (7) "Consent" means a clear affirmative act signifying a
36 consumer's freely given, specific, informed and unambiguous

37 agreement to allow the processing of personal data relating to the
38 consumer. "Consent" may include a written statement, including by
39 electronic means, or any other unambiguous affirmative action.
40 "Consent" does not include (A) acceptance of a general or broad terms
41 of use or similar document that contains descriptions of personal data
42 processing along with other, unrelated information, (B) hovering over,
43 muting, pausing or closing a given piece of content, or (C) agreement
44 obtained through the use of dark patterns.

45 [(7)] (8) "Consumer" means an individual who is a resident of this
46 state. "Consumer" does not include an individual acting in a commercial
47 or employment context or as an employee, owner, director, officer or
48 contractor of a company, partnership, sole proprietorship, nonprofit or
49 government agency whose communications or transactions with the
50 controller occur solely within the context of that individual's role with
51 the company, partnership, sole proprietorship, nonprofit or government
52 agency.

53 (9) "Consumer health data" means any personal data that a controller
54 uses to identify a consumer's physical or mental health condition or
55 diagnosis, and includes, but is not limited to, gender-affirming health
56 data and reproductive or sexual health data.

57 (10) "Consumer health data controller" means any controller that,
58 alone or jointly with others, determines the purpose and means of
59 processing consumer health data.

60 [(8)] (11) "Controller" means [an individual] a person who, [or legal
61 entity that,] alone or jointly with others, determines the purpose and
62 means of processing personal data.

63 [(9)] (12) "COPPA" means the Children's Online Privacy Protection
64 Act of 1998, 15 USC 6501 et seq., and the regulations, rules, guidance
65 and exemptions adopted pursuant to said act, as said act and such
66 regulations, rules, guidance and exemptions may be amended from
67 time to time.

68 [(10)] (13) "Covered entity" has the same meaning as provided in
69 HIPAA.

70 [(11)] (14) "Dark pattern" [(A)] means a user interface designed or
71 manipulated with the substantial effect of subverting or impairing user
72 autonomy, decision-making or choice, and [(B)] includes, but is not
73 limited to, any practice the Federal Trade Commission refers to as a
74 "dark pattern".

75 [(12)] (15) "Decisions that produce legal or similarly significant effects
76 concerning the consumer" means decisions made by the controller that
77 result in the provision or denial by the controller of financial or lending
78 services, housing, insurance, education enrollment or opportunity,
79 criminal justice, employment opportunities, health care services or
80 access to essential goods or services.

81 [(13)] (16) "De-identified data" means data that cannot reasonably be
82 used to infer information about, or otherwise be linked to, an identified
83 or identifiable individual, or a device linked to such individual, if the
84 controller that possesses such data (A) takes reasonable measures to
85 ensure that such data cannot be associated with an individual, (B)
86 publicly commits to process such data only in a de-identified fashion
87 and not attempt to re-identify such data, and (C) contractually obligates
88 any recipients of such data to satisfy the criteria set forth in
89 subparagraphs (A) and (B) of this subdivision.

90 (17) "Gender-affirming health care services" has the same meaning as
91 provided in section 52-571n.

92 (18) "Gender-affirming health data" means any personal data
93 concerning an effort made by a consumer to seek, or a consumer's
94 receipt of, gender-affirming health care services.

95 (19) "Geofence" means any technology that uses global positioning
96 coordinates, cell tower connectivity, cellular data, radio frequency
97 identification, wireless fidelity technology data or any other form of
98 location detection, or any combination of such coordinates, connectivity,

99 data, identification or other form of location detection, to establish a
100 virtual boundary.

101 [(14)] (20) "HIPAA" means the Health Insurance Portability and
102 Accountability Act of 1996, 42 USC 1320d et seq., as amended from time
103 to time.

104 [(15)] (21) "Identified or identifiable individual" means an individual
105 who can be readily identified, directly or indirectly.

106 [(16)] (22) "Institution of higher education" means any individual
107 who, or school, board, association, limited liability company or
108 corporation that, is licensed or accredited to offer one or more programs
109 of higher learning leading to one or more degrees.

110 (23) "Mental health facility" means any health care facility in which at
111 least seventy per cent of the health care services provided in such facility
112 are mental health services.

113 [(17)] (24) "Nonprofit organization" means any organization that is
114 exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or
115 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent
116 corresponding internal revenue code of the United States, as amended
117 from time to time.

118 (25) "Person" means an individual, association, company, limited
119 liability company, corporation, partnership, sole proprietorship, trust or
120 other legal entity.

121 [(18)] (26) "Personal data" means any information that is linked or
122 reasonably linkable to an identified or identifiable individual. "Personal
123 data" does not include de-identified data or publicly available
124 information.

125 [(19)] (27) "Precise geolocation data" means information derived from
126 technology, including, but not limited to, global positioning system
127 level latitude and longitude coordinates or other mechanisms, that
128 directly identifies the specific location of an individual with precision

129 and accuracy within a radius of one thousand seven hundred fifty feet.
130 "Precise geolocation data" does not include the content of
131 communications or any data generated by or connected to advanced
132 utility metering infrastructure systems or equipment for use by a utility.

133 [(20)] (28) "Process" [or] and "processing" [means] mean any
134 operation or set of operations performed, whether by manual or
135 automated means, on personal data or on sets of personal data, such as
136 the collection, use, storage, disclosure, analysis, deletion or modification
137 of personal data.

138 [(21)] (29) "Processor" means [an individual] a person who [, or legal
139 entity that,] processes personal data on behalf of a controller.

140 [(22)] (30) "Profiling" means any form of automated processing
141 performed on personal data to evaluate, analyze or predict personal
142 aspects related to an identified or identifiable individual's economic
143 situation, health, personal preferences, interests, reliability, behavior,
144 location or movements.

145 [(23)] (31) "Protected health information" has the same meaning as
146 provided in HIPAA.

147 [(24)] (32) "Pseudonymous data" means personal data that cannot be
148 attributed to a specific individual without the use of additional
149 information, provided such additional information is kept separately
150 and is subject to appropriate technical and organizational measures to
151 ensure that the personal data is not attributed to an identified or
152 identifiable individual.

153 [(25)] (33) "Publicly available information" means information that
154 (A) is lawfully made available through federal, state or municipal
155 government records or widely distributed media, and (B) a controller
156 has a reasonable basis to believe a consumer has lawfully made
157 available to the general public.

158 (34) "Reproductive or sexual health care" means any health care-

159 related services or products rendered or provided concerning a
160 consumer's reproductive system or sexual well-being, including, but not
161 limited to, any such service or product rendered or provided concerning
162 (A) an individual health condition, status, disease, diagnosis, diagnostic
163 test or treatment, (B) a social, psychological, behavioral or medical
164 intervention, (C) a surgery or procedure, including, but not limited to,
165 an abortion, (D) a use or purchase of a medication, including, but not
166 limited to, a medication used or purchased for the purposes of an
167 abortion, (E) a bodily function, vital sign or symptom, (F) a
168 measurement of a bodily function, vital sign or symptom, or (G) an
169 abortion, including, but not limited to, medical or nonmedical services,
170 products, diagnostics, counseling or follow-up services for an abortion.

171 (35) "Reproductive or sexual health data" means any personal data
172 concerning an effort made by a consumer to seek, or a consumer's
173 receipt of, reproductive or sexual health care.

174 (36) "Reproductive or sexual health facility" means any health care
175 facility in which at least seventy per cent of the health care-related
176 services or products rendered or provided in such facility are
177 reproductive or sexual health care.

178 ~~[(26)]~~ (37) "Sale of personal data" means the exchange of personal data
179 for monetary or other valuable consideration by the controller to a third
180 party. "Sale of personal data" does not include (A) the disclosure of
181 personal data to a processor that processes the personal data on behalf
182 of the controller, (B) the disclosure of personal data to a third party for
183 purposes of providing a product or service requested by the consumer,
184 (C) the disclosure or transfer of personal data to an affiliate of the
185 controller, (D) the disclosure of personal data where the consumer
186 directs the controller to disclose the personal data or intentionally uses
187 the controller to interact with a third party, (E) the disclosure of personal
188 data that the consumer (i) intentionally made available to the general
189 public via a channel of mass media, and (ii) did not restrict to a specific
190 audience, or (F) the disclosure or transfer of personal data to a third
191 party as an asset that is part of a merger, acquisition, bankruptcy or

192 other transaction, or a proposed merger, acquisition, bankruptcy or
193 other transaction, in which the third party assumes control of all or part
194 of the controller's assets.

195 [(27)] (38) "Sensitive data" means personal data that includes (A) data
196 revealing racial or ethnic origin, religious beliefs, mental or physical
197 health condition or diagnosis, sex life, sexual orientation or citizenship
198 or immigration status, (B) consumer health data, (C) the processing of
199 genetic or biometric data for the purpose of uniquely identifying an
200 individual, [(C)] (D) personal data collected from a known child, [or (D)]
201 (E) data concerning an individual's status as a victim of crime, as defined
202 in section 1-1k, or (F) precise geolocation data.

203 [(28)] (39) "Targeted advertising" means displaying advertisements to
204 a consumer where the advertisement is selected based on personal data
205 obtained or inferred from that consumer's activities over time and across
206 nonaffiliated Internet web sites or online applications to predict such
207 consumer's preferences or interests. "Targeted advertising" does not
208 include (A) advertisements based on activities within a controller's own
209 Internet web sites or online applications, (B) advertisements based on
210 the context of a consumer's current search query, visit to an Internet web
211 site or online application, (C) advertisements directed to a consumer in
212 response to the consumer's request for information or feedback, or (D)
213 processing personal data solely to measure or report advertising
214 frequency, performance or reach.

215 [(29)] (40) "Third party" means [an individual or legal entity] a
216 person, such as a public authority, agency or body, other than the
217 consumer, controller or processor or an affiliate of the processor or the
218 controller.

219 [(30)] (41) "Trade secret" has the same meaning as provided in section
220 35-51.

221 Sec. 2. (NEW) (*Effective July 1, 2023*) (a) (1) Except as provided in
222 subsection (b) of this section, subsections (b) and (c) of section 42-517 of
223 the general statutes, as amended by this act, and section 42-524 of the

224 general statutes, as amended by this act, no person shall: (A) Provide
225 any employee or contractor with access to consumer health data unless
226 the employee or contractor is subject to a contractual or statutory duty
227 of confidentiality; (B) provide any processor with access to consumer
228 health data unless such person and processor comply with section 42-
229 521 of the general statutes; (C) use a geofence to establish a virtual
230 boundary that is within one thousand seven hundred fifty feet of any
231 mental health facility or reproductive or sexual health facility for the
232 purpose of identifying, tracking, collecting data from or sending any
233 notification to a consumer regarding the consumer's consumer health
234 data; or (D) sell, or offer to sell, consumer health data without first
235 obtaining the consumer's consent.

236 (2) Notwithstanding section 42-516 of the general statutes, the
237 provisions of subsection (a) of this section, and the provisions of section
238 42-515, as amended by this act, and sections 42-517 to 42-525, inclusive,
239 of the general statutes, as amended by this act, concerning consumer
240 health data and consumer health data controllers, apply to persons that
241 conduct business in this state and persons that produce products or
242 services that are targeted to residents of this state.

243 (b) The provisions of subsection (a) of this section shall not apply to
244 any: (1) Body, authority, board, bureau, commission, district or agency
245 of this state or of any political subdivision of this state; (2) person who
246 has entered into a contract with any body, authority, board, bureau,
247 commission, district or agency described in subdivision (1) of this
248 subsection while such person is processing consumer health data on
249 behalf of such body, authority, board, bureau, commission, district or
250 agency pursuant to such contract; (3) institution of higher education; (4)
251 national securities association that is registered under 15 USC 78o-3 of
252 the Securities Exchange Act of 1934, as amended from time to time; (5)
253 financial institution or data subject to Title V of the Gramm-Leach-Bliley
254 Act, 15 USC 6801 et seq.; (6) covered entity or business associate, as
255 defined in 45 CFR 160.103; (7) tribal nation government organization; or
256 (8) air carrier, as defined in 49 USC 40102, as amended from time to time,
257 and regulated under the Federal Aviation Act of 1958, 49 USC 40101 et

258 seq., and the Airline Deregulation Act of 1978, 49 USC 41713, as said acts
259 may be amended from time to time.

260 Sec. 3. Subsections (a) to (c), inclusive, of section 42-517 of the general
261 statutes are repealed and the following is substituted in lieu thereof
262 (*Effective July 1, 2023*):

263 (a) The provisions of sections 42-515 to 42-525, inclusive, as amended
264 by this act, do not apply to any: (1) Body, authority, board, bureau,
265 commission, district or agency of this state or of any political
266 subdivision of this state; (2) person who has entered into a contract with
267 any body, authority, board, bureau, commission, district or agency
268 described in subdivision (1) of this subsection while such person is
269 processing consumer health data on behalf of such body, authority,
270 board, bureau, commission, district or agency pursuant to such contract;
271 (3) nonprofit organization; [(3)] (4) institution of higher education; [(4)]
272 (5) national securities association that is registered under 15 USC 78o-3
273 of the Securities Exchange Act of 1934, as amended from time to time;
274 [(5)] (6) financial institution or data subject to Title V of the Gramm-
275 Leach-Bliley Act, 15 USC 6801 et seq.; [or (6)] (7) covered entity or
276 business associate, as defined in 45 CFR 160.103; (8) tribal nation
277 government organization; or (9) air carrier, as defined in 49 USC 40102,
278 as amended from time to time, and regulated under the Federal
279 Aviation Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation
280 Act of 1978, 49 USC 41713, as said acts may be amended from time to
281 time.

282 (b) The following information and data is exempt from the provisions
283 of sections 42-515 to 42-525, inclusive, as amended by this act, and
284 section 2 of this act: (1) Protected health information under HIPAA; (2)
285 patient-identifying information for purposes of 42 USC 290dd-2; (3)
286 identifiable private information for purposes of the federal policy for the
287 protection of human subjects under 45 CFR 46; (4) identifiable private
288 information that is otherwise information collected as part of human
289 subjects research pursuant to the good clinical practice guidelines issued
290 by the International Council for Harmonization of Technical

291 Requirements for Pharmaceuticals for Human Use; (5) the protection of
292 human subjects under 21 CFR Parts 6, 50 and 56, or personal data used
293 or shared in research, as defined in 45 CFR 164.501, that is conducted in
294 accordance with the standards set forth in this subdivision and
295 subdivisions (3) and (4) of this subsection, or other research conducted
296 in accordance with applicable law; (6) information and documents
297 created for purposes of the Health Care Quality Improvement Act of
298 1986, 42 USC 11101 et seq.; (7) patient safety work product for purposes
299 of section 19a-127o and the Patient Safety and Quality Improvement
300 Act, 42 USC 299b-21 et seq., as amended from time to time; (8)
301 information derived from any of the health [care related] care-related
302 information listed in this subsection that is de-identified in accordance
303 with the requirements for de-identification pursuant to HIPAA; (9)
304 information originating from and intermingled to be indistinguishable
305 with, or information treated in the same manner as, information exempt
306 under this subsection that is maintained by a covered entity or business
307 associate, program or qualified service organization, as specified in 42
308 USC 290dd-2, as amended from time to time; (10) information used for
309 public health activities and purposes as authorized by HIPAA,
310 community health activities and population health activities; (11) the
311 collection, maintenance, disclosure, sale, communication or use of any
312 personal information bearing on a consumer's credit worthiness, credit
313 standing, credit capacity, character, general reputation, personal
314 characteristics or mode of living by a consumer reporting agency,
315 furnisher or user that provides information for use in a consumer report,
316 and by a user of a consumer report, but only to the extent that such
317 activity is regulated by and authorized under the Fair Credit Reporting
318 Act, 15 USC 1681 et seq., as amended from time to time; (12) personal
319 data collected, processed, sold or disclosed in compliance with the
320 Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., as amended
321 from time to time; (13) personal data regulated by the Family
322 Educational Rights and Privacy Act, 20 USC 1232g et seq., as amended
323 from time to time; (14) personal data collected, processed, sold or
324 disclosed in compliance with the Farm Credit Act, 12 USC 2001 et seq.,
325 as amended from time to time; (15) data processed or maintained (A) in

326 the course of an individual applying to, employed by or acting as an
327 agent or independent contractor of a controller, processor, consumer
328 health data controller or third party, to the extent that the data is
329 collected and used within the context of that role, (B) as the emergency
330 contact information of an individual under sections 42-515 to 42-525,
331 inclusive, as amended by this act, and section 2 of this act used for
332 emergency contact purposes, or (C) that is necessary to retain to
333 administer benefits for another individual relating to the individual
334 who is the subject of the information under subdivision (1) of this
335 subsection and used for the purposes of administering such benefits;
336 and (16) personal data collected, processed, sold or disclosed in relation
337 to price, route or service, as such terms are used in the [Airline
338 Deregulation Act] Federal Aviation Act of 1958, 49 USC 40101 et seq.,
339 [as amended from time to time, by an air carrier subject to said act, to
340 the extent sections 42-515 to 42-525, inclusive, are preempted by] and
341 the Airline Deregulation Act of 1978, 49 USC 41713, as said acts may be
342 amended from time to time.

343 (c) Controllers, [and] processors and consumer health data
344 controllers that comply with the verifiable parental consent
345 requirements of COPPA shall be deemed compliant with any obligation
346 to obtain parental consent pursuant to sections 42-515 to 42-525,
347 inclusive, as amended by this act, and section 2 of this act.

348 Sec. 4. Subsection (a) of section 42-520 of the general statutes is
349 repealed and the following is substituted in lieu thereof (*Effective July 1,*
350 *2023*):

351 (a) A controller shall: (1) Limit the collection of personal data to what
352 is adequate, relevant and reasonably necessary in relation to the
353 purposes for which such data is processed, as disclosed to the consumer;
354 (2) except as otherwise provided in sections 42-515 to 42-525, inclusive,
355 as amended by this act, not process personal data for purposes that are
356 neither reasonably necessary to, nor compatible with, the disclosed
357 purposes for which such personal data is processed, as disclosed to the
358 consumer, unless the controller obtains the consumer's consent; (3)

359 establish, implement and maintain reasonable administrative, technical
360 and physical data security practices to protect the confidentiality,
361 integrity and accessibility of personal data appropriate to the volume
362 and nature of the personal data at issue; (4) not process sensitive data
363 concerning a consumer without obtaining the consumer's consent, or, in
364 the case of the processing of sensitive data concerning a known child,
365 without processing such data in accordance with COPPA; (5) not
366 process personal data in violation of the laws of this state and federal
367 laws that prohibit unlawful discrimination against consumers; (6)
368 provide an effective mechanism for a consumer to revoke the
369 consumer's consent under this section that is at least as easy as the
370 mechanism by which the consumer provided the consumer's consent
371 and, upon revocation of such consent, cease to process the data as soon
372 as practicable, but not later than fifteen days after the receipt of such
373 request; and (7) not process the personal data of a consumer for
374 purposes of targeted advertising, or sell the consumer's personal data
375 without the consumer's consent, under circumstances where a controller
376 has actual knowledge, [and] or wilfully disregards, that the consumer is
377 at least thirteen years of age but younger than sixteen years of age. A
378 controller shall not discriminate against a consumer for exercising any
379 of the consumer rights contained in sections 42-515 to 42-525, inclusive,
380 as amended by this act, including denying goods or services, charging
381 different prices or rates for goods or services or providing a different
382 level of quality of goods or services to the consumer.

383 Sec. 5. Section 42-524 of the general statutes is repealed and the
384 following is substituted in lieu thereof (*Effective July 1, 2023*):

385 (a) Nothing in sections 42-515 to 42-525, inclusive, as amended by this
386 act, or section 2 of this act shall be construed to restrict a controller's, [or]
387 processor's or consumer health data controller's ability to: (1) Comply
388 with federal, state or municipal ordinances or regulations; (2) comply
389 with a civil, criminal or regulatory inquiry, investigation, subpoena or
390 summons by federal, state, municipal or other governmental
391 authorities; (3) cooperate with law enforcement agencies concerning
392 conduct or activity that the controller, [or] processor or consumer health

393 data controller reasonably and in good faith believes may violate
394 federal, state or municipal ordinances or regulations; (4) investigate,
395 establish, exercise, prepare for or defend legal claims; (5) provide a
396 product or service specifically requested by a consumer; (6) perform
397 under a contract to which a consumer is a party, including fulfilling the
398 terms of a written warranty; (7) take steps at the request of a consumer
399 prior to entering into a contract; (8) take immediate steps to protect an
400 interest that is essential for the life or physical safety of the consumer or
401 another individual, and where the processing cannot be manifestly
402 based on another legal basis; (9) prevent, detect, protect against or
403 respond to security incidents, identity theft, fraud, harassment,
404 malicious or deceptive activities or any illegal activity, preserve the
405 integrity or security of systems or investigate, report or prosecute those
406 responsible for any such action; (10) engage in public or peer-reviewed
407 scientific or statistical research in the public interest that adheres to all
408 other applicable ethics and privacy laws and is approved, monitored
409 and governed by an institutional review board that determines, or
410 similar independent oversight entities that determine, (A) whether the
411 deletion of the information is likely to provide substantial benefits that
412 do not exclusively accrue to the controller or consumer health data
413 controller, (B) the expected benefits of the research outweigh the privacy
414 risks, and (C) whether the controller or consumer health data controller
415 has implemented reasonable safeguards to mitigate privacy risks
416 associated with research, including any risks associated with re-
417 identification; (11) assist another controller, processor, consumer health
418 data controller or third party with any of the obligations under sections
419 42-515 to 42-525, inclusive, as amended by this act, or section 2 of this
420 act; or (12) process personal data for reasons of public interest in the area
421 of public health, community health or population health, but solely to
422 the extent that such processing is (A) subject to suitable and specific
423 measures to safeguard the rights of the consumer whose personal data
424 is being processed, and (B) under the responsibility of a professional
425 subject to confidentiality obligations under federal, state or local law.

426 (b) The obligations imposed on controllers, [or] processors or

427 consumer health data controllers under sections 42-515 to 42-525,
428 inclusive, as amended by this act, and section 2 of this act shall not
429 restrict a controller's, [or] processor's or consumer health data
430 controller's ability to collect, use or retain data for internal use to: (1)
431 Conduct internal research to develop, improve or repair products,
432 services or technology; (2) effectuate a product recall; (3) identify and
433 repair technical errors that impair existing or intended functionality; or
434 (4) perform internal operations that are reasonably aligned with the
435 expectations of the consumer or reasonably anticipated based on the
436 consumer's existing relationship with the controller or consumer health
437 data controller, or are otherwise compatible with processing data in
438 furtherance of the provision of a product or service specifically
439 requested by a consumer or the performance of a contract to which the
440 consumer is a party.

441 (c) The obligations imposed on controllers, [or] processors or
442 consumer health data controllers under sections 42-515 to 42-525,
443 inclusive, as amended by this act, and section 2 of this act shall not apply
444 where compliance by the controller, [or] processor or consumer health
445 data controller with said sections would violate an evidentiary privilege
446 under the laws of this state. Nothing in sections 42-515 to 42-525,
447 inclusive, as amended by this act, or section 2 of this act shall be
448 construed to prevent a controller, [or] processor or consumer health data
449 controller from providing personal data concerning a consumer to a
450 person covered by an evidentiary privilege under the laws of the state
451 as part of a privileged communication.

452 (d) A controller, [or] processor or consumer health data controller
453 that discloses personal data to a processor or third-party controller in
454 accordance with sections 42-515 to 42-525, inclusive, as amended by this
455 act, and section 2 of this act shall not be deemed to have violated said
456 sections if the processor or third-party controller that receives and
457 processes such personal data violates said sections, provided, at the time
458 the disclosing controller, [or] processor or consumer health data
459 controller disclosed such personal data, the disclosing controller, [or]
460 processor or consumer health data controller did not have actual

461 knowledge that the receiving processor or third-party controller would
462 violate said sections. A third-party controller or processor receiving
463 personal data from a controller, [or] processor or consumer health data
464 controller in compliance with sections 42-515 to 42-525, inclusive, as
465 amended by this act, and section 2 of this act is likewise not in violation
466 of said sections for the transgressions of the controller, [or] processor or
467 consumer health data controller from which such third-party controller
468 or processor receives such personal data.

469 (e) Nothing in sections 42-515 to 42-525, inclusive, as amended by this
470 act, or section 2 of this act shall be construed to: (1) Impose any
471 obligation on a controller, [or] processor or consumer health data
472 controller that adversely affects the rights or freedoms of any person,
473 including, but not limited to, the rights of any person (A) to freedom of
474 speech or freedom of the press guaranteed in the First Amendment to
475 the United States Constitution, or (B) under section 52-146t; or (2) apply
476 to any person's processing of personal data in the course of such
477 person's purely personal or household activities.

478 (f) Personal data processed by a controller or consumer health data
479 controller pursuant to this section may be processed to the extent that
480 such processing is: (1) Reasonably necessary and proportionate to the
481 purposes listed in this section; and (2) adequate, relevant and limited to
482 what is necessary in relation to the specific purposes listed in this
483 section. Personal data collected, used or retained pursuant to subsection
484 (b) of this section shall, where applicable, take into account the nature
485 and purpose or purposes of such collection, use or retention. Such data
486 shall be subject to reasonable administrative, technical and physical
487 measures to protect the confidentiality, integrity and accessibility of the
488 personal data and to reduce reasonably foreseeable risks of harm to
489 consumers relating to such collection, use or retention of personal data.

490 (g) If a controller or consumer health data controller processes
491 personal data pursuant to an exemption in this section, the controller or
492 consumer health data controller bears the burden of demonstrating that
493 such processing qualifies for the exemption and complies with the

494 requirements in subsection (f) of this section.

495 (h) Processing personal data for the purposes expressly identified in
496 this section shall not solely make a legal entity a controller or consumer
497 health data controller with respect to such processing.

498 Sec. 6. Section 42-525 of the general statutes is repealed and the
499 following is substituted in lieu thereof (*Effective July 1, 2023*):

500 (a) The Attorney General shall have exclusive authority to enforce
501 violations of sections 42-515 to 42-524, inclusive, as amended by this act,
502 and section 2 of this act.

503 (b) During the period beginning on July 1, 2023, and ending on
504 December 31, 2024, the Attorney General shall, prior to initiating any
505 action for a violation of any provision of sections 42-515 to 42-524,
506 inclusive, as amended by this act, and section 2 of this act, issue a notice
507 of violation to the controller or consumer health data controller if the
508 Attorney General determines that a cure is possible. If the controller or
509 consumer health data controller fails to cure such violation within sixty
510 days of receipt of the notice of violation, the Attorney General may bring
511 an action pursuant to this section. Not later than February 1, 2024, the
512 Attorney General shall submit a report, in accordance with section 11-
513 4a, to the joint standing committee of the General Assembly having
514 cognizance of matters relating to general law disclosing: (1) The number
515 of notices of violation the Attorney General has issued; (2) the nature of
516 each violation; (3) the number of violations that were cured during the
517 sixty-day cure period; and (4) any other matter the Attorney General
518 deems relevant for the purposes of such report.

519 (c) Beginning on January 1, 2025, the Attorney General may, in
520 determining whether to grant a controller, [or] processor or consumer
521 health data controller the opportunity to cure an alleged violation
522 described in subsection (b) of this section, consider: (1) The number of
523 violations; (2) the size and complexity of the controller, [or] processor or
524 consumer health data controller; (3) the nature and extent of the
525 controller's, [or] processor's or consumer health data controller's

526 processing activities; (4) the substantial likelihood of injury to the public;
527 (5) the safety of persons or property; [and] (6) whether such alleged
528 violation was likely caused by human or technical error; and (7) the
529 sensitivity of the data.

530 (d) Nothing in sections 42-515 to 42-524, inclusive, as amended by this
531 act, or section 2 of this act shall be construed as providing the basis for,
532 or be subject to, a private right of action for violations of said sections or
533 any other law.

534 (e) A violation of the requirements of sections 42-515 to 42-524,
535 inclusive, as amended by this act, or section 2 of this act shall constitute
536 an unfair trade practice for purposes of section 42-110b and shall be
537 enforced solely by the Attorney General, provided the provisions of
538 section 42-110g shall not apply to such violation.

539 Sec. 7. (NEW) (*Effective July 1, 2024*) (a) For the purposes of this
540 section:

541 (1) "Authenticate" means to use reasonable means and make a
542 commercially reasonable effort to determine whether a request to
543 exercise any right afforded under subsection (b) of this section has been
544 submitted by, or on behalf of, the minor who is entitled to exercise such
545 right;

546 (2) "Consumer" has the same meaning as provided in section 42-515
547 of the general statutes, as amended by this act;

548 (3) "Minor" means any consumer who is younger than eighteen years
549 of age;

550 (4) "Personal data" has the same meaning as provided in section 42-
551 515 of the general statutes, as amended by this act;

552 (5) "Social media platform" (A) means a public or semi-public
553 Internet-based service or application that (i) is used by a consumer in
554 this state, (ii) is primarily intended to connect and allow users to socially
555 interact within such service or application, and (iii) enables a user to (I)

556 construct a public or semi-public profile for the purposes of signing into
557 and using such service or application, (II) populate a public list of other
558 users with whom the user shares a social connection within such service
559 or application, and (III) create or post content that is viewable by other
560 users, including, but not limited to, on message boards, in chat rooms,
561 or through a landing page or main feed that presents the user with
562 content generated by other users, and (B) does not include a public or
563 semi-public Internet-based service or application that (i) exclusively
564 provides electronic mail or direct messaging services, (ii) primarily
565 consists of news, sports, entertainment, interactive video games,
566 electronic commerce or content that is preselected by the provider or for
567 which any chat, comments or interactive functionality is incidental to,
568 directly related to, or dependent on the provision of such content, or (iii)
569 is used by and under the direction of an educational entity, including,
570 but not limited to, a learning management system or a student
571 engagement program; and

572 (6) "Unpublish" means to remove a social media platform account
573 from public visibility.

574 (b) (1) Not later than fifteen business days after a social media
575 platform receives a request from a minor or, if the minor is younger than
576 sixteen years of age, from such minor's parent or legal guardian to
577 unpublish such minor's social media platform account, the social media
578 platform shall unpublish such minor's social media platform account.

579 (2) Not later than forty-five business days after a social media
580 platform receives a request from a minor or, if the minor is younger than
581 sixteen years of age, from such minor's parent or legal guardian to delete
582 such minor's social media platform account, the social media platform
583 shall delete such minor's social media platform account and cease
584 processing such minor's personal data except where the preservation of
585 such minor's social media platform account or personal data is
586 otherwise permitted or required by applicable law, including, but not
587 limited to, sections 42-515 to 42-525, inclusive, of the general statutes, as
588 amended by this act. A social media platform may extend such forty-

589 five business day period by an additional forty-five business days if
590 such extension is reasonably necessary considering the complexity and
591 number of the consumer's requests, provided the social media platform
592 informs the minor or, if the minor is younger than sixteen years of age,
593 such minor's parent or legal guardian within the initial forty-five
594 business day response period of such extension and the reason for such
595 extension.

596 (3) A social media platform shall establish, and shall describe in a
597 privacy notice, one or more secure and reliable means for submitting a
598 request pursuant to this subsection. A social media platform that
599 provides a mechanism for a minor or, if the minor is younger than
600 sixteen years of age, the minor's parent or legal guardian to initiate a
601 process to delete or unpublish such minor's social media platform
602 account shall be deemed to be in compliance with the provisions of this
603 subsection.

604 (c) If a social media platform is unable to authenticate a request
605 submitted under subsection (b) of this section, the social media platform
606 shall (1) not be required to comply with such request, and (2) provide a
607 notice to the consumer who submitted such request disclosing that such
608 social media platform (A) is unable to authenticate such request, and (B)
609 will not be able to authenticate such request until such consumer
610 provides the additional information that is reasonably necessary to
611 authenticate such request.

612 (d) Any violation of the provisions of this section shall constitute an
613 unfair trade practice under subsection (a) of section 42-110b of the
614 general statutes and shall be enforced solely by the Attorney General.
615 Nothing in this section shall be construed to create a private right of
616 action or to provide grounds for an action under section 42-110g of the
617 general statutes.

618 Sec. 8. (NEW) (*Effective October 1, 2024*) For the purposes of this
619 section and sections 9 to 13, inclusive, of this act:

620 (1) "Adult" means any individual who is at least eighteen years of age;

621 (2) "Consent" has the same meaning as provided in section 42-515 of
622 the general statutes, as amended by this act;

623 (3) "Consumer" has the same meaning as provided in section 42-515
624 of the general statutes, as amended by this act;

625 (4) "Controller" has the same meaning as provided in section 42-515
626 of the general statutes, as amended by this act;

627 (5) "Heightened risk of harm to minors" means processing minors'
628 personal data in a manner that presents any reasonably foreseeable risk
629 of (A) any unfair or deceptive treatment of, or any unlawful disparate
630 impact on, minors, (B) any financial, physical or reputational injury to
631 minors, or (C) any physical or other intrusion upon the solitude or
632 seclusion, or the private affairs or concerns, of minors if such intrusion
633 would be offensive to a reasonable person;

634 (6) "HIPAA" has the same meaning as provided in section 42-515 of
635 the general statutes, as amended by this act;

636 (7) "Minor" means any consumer who is younger than eighteen years
637 of age;

638 (8) "Online service, product or feature" means any service, product or
639 feature that is provided online. "Online service, product or feature" does
640 not include any (A) telecommunications service, as defined in 47 USC
641 153, as amended from time to time, (B) broadband Internet access
642 service, as defined in 47 CFR 54.400, as amended from time to time, or
643 (C) delivery or use of a physical product;

644 (9) "Person" has the same meaning as provided in section 42-515 of
645 the general statutes, as amended by this act;

646 (10) "Personal data" has the same meaning as provided in section 42-
647 515 of the general statutes, as amended by this act;

648 (11) "Precise geolocation data" has the same meaning as provided in
649 section 42-515 of the general statutes, as amended by this act;

650 (12) "Process" and "processing" have the same meaning as provided
651 in section 42-515 of the general statutes, as amended by this act;

652 (13) "Processor" has the same meaning as provided in section 42-515
653 of the general statutes, as amended by this act;

654 (14) "Profiling" has the same meaning as provided in section 42-515
655 of the general statutes, as amended by this act;

656 (15) "Protected health information" has the same meaning as
657 provided in section 42-515 of the general statutes, as amended by this
658 act;

659 (16) "Sale of personal data" has the same meaning as provided in
660 section 42-515 of the general statutes, as amended by this act;

661 (17) "Targeted advertising" has the same meaning as provided in
662 section 42-515 of the general statutes, as amended by this act; and

663 (18) "Third party" has the same meaning as provided in section 42-
664 515 of the general statutes, as amended by this act.

665 Sec. 9. (NEW) (*Effective October 1, 2024*) (a) Each controller that offers
666 any online service, product or feature to consumers whom such
667 controller has actual knowledge, or wilfully disregards, are minors shall
668 use reasonable care to avoid any heightened risk of harm to minors
669 caused by such online service, product or feature. In any enforcement
670 action brought by the Attorney General pursuant to section 13 of this
671 act, there shall be a rebuttable presumption that a controller used
672 reasonable care as required under this section if the controller complied
673 with the provisions of section 10 of this act concerning data protection
674 assessments.

675 (b) (1) Subject to the consent requirement established in subdivision
676 (3) of this subsection, no controller that offers any online service,
677 product or feature to consumers whom such controller has actual
678 knowledge, or wilfully disregards, are minors shall: (A) Process any
679 minor's personal data (i) for the purposes of (I) targeted advertising, (II)

680 any sale of personal data, or (III) profiling in furtherance of any fully
681 automated decision made by such controller that produces any legal or
682 similarly significant effect concerning the provision or denial by such
683 controller of any financial or lending services, housing, insurance,
684 education enrollment or opportunity, criminal justice, employment
685 opportunity, health care services or access to essential goods or services,
686 (ii) unless such processing is reasonably necessary to provide such
687 online service, product or feature, (iii) for any processing purpose (I)
688 other than the processing purpose that the controller disclosed at the
689 time such controller collected such personal data, or (II) that is
690 reasonably necessary for, and compatible with, the processing purpose
691 described in subparagraph (A)(iii)(I) of this subdivision, or (iv) for
692 longer than is reasonably necessary to provide such online service,
693 product or feature; or (B) use any system design feature to significantly
694 increase, sustain or extend any minor's use of such online service,
695 product or feature. The provisions of this subdivision shall not apply to
696 any service or application that is used by and under the direction of an
697 educational entity, including, but not limited to, a learning management
698 system or a student engagement program.

699 (2) Subject to the consent requirement established in subdivision (3)
700 of this subsection, no controller that offers an online service, product or
701 feature to consumers whom such controller has actual knowledge, or
702 wilfully disregards, are minors shall collect a minor's precise
703 geolocation data unless: (A) Such precise geolocation data is reasonably
704 necessary for the controller to provide such online service, product or
705 feature and, if such data is necessary to provide such online service,
706 product or feature, such controller may only collect such data for the
707 time necessary to provide such online service, product or feature; and
708 (B) the controller provides to the minor a signal indicating that such
709 controller is collecting such precise geolocation data, which signal shall
710 be available to such minor for the entire duration of such collection.

711 (3) No controller shall engage in the activities described in
712 subdivisions (1) and (2) of this subsection unless the controller obtains
713 the minor's consent or, if the minor is younger than thirteen years of age,

714 the consent of such minor's parent or legal guardian. A controller that
715 complies with the verifiable parental consent requirements established
716 in the Children's Online Privacy Protection Act of 1998, 15 USC 6501 et
717 seq., and the regulations, rules, guidance and exemptions adopted
718 pursuant to said act, as said act and such regulations, rules, guidance
719 and exemptions may be amended from time to time, shall be deemed to
720 have satisfied any requirement to obtain parental consent under this
721 subdivision.

722 (c) (1) No controller that offers any online service, product or feature
723 to consumers whom such controller has actual knowledge, or wilfully
724 disregards, are minors shall: (A) Provide any consent mechanism that is
725 designed to substantially subvert or impair, or is manipulated with the
726 effect of substantially subverting or impairing, user autonomy, decision-
727 making or choice; or (B) except as provided in subdivision (2) of this
728 subsection, offer any direct messaging apparatus for use by minors
729 without providing readily accessible and easy-to-use safeguards to limit
730 the ability of adults to send unsolicited communications to minors with
731 whom they are not connected.

732 (2) The provisions of subparagraph (B) of subdivision (1) of this
733 subsection shall not apply to services where the predominant or
734 exclusive function is: (A) Electronic mail; or (B) direct messaging
735 consisting of text, photos or videos that are sent between devices by
736 electronic means, where messages are (i) shared between the sender and
737 the recipient, (ii) only visible to the sender and the recipient, and (iii) not
738 posted publicly.

739 Sec. 10. (NEW) (*Effective October 1, 2024*) (a) Each controller that, on
740 or after October 1, 2024, offers any online service, product or feature to
741 consumers whom such controller has actual knowledge, or wilfully
742 disregards, are minors shall conduct a data protection assessment for
743 such online service, product or feature: (1) In a manner that is consistent
744 with the requirements established in section 42-522 of the general
745 statutes; and (2) that addresses (A) the purpose of such online service,
746 product or feature, (B) the categories of minors' personal data that such

747 online service, product or feature processes, (C) the purposes for which
748 such controller processes minors' personal data with respect to such
749 online service, product or feature, and (D) any heightened risk of harm
750 to minors that is a reasonably foreseeable result of offering such online
751 service, product or feature to minors.

752 (b) Each controller that conducts a data protection assessment
753 pursuant to subsection (a) of this section shall: (1) Review such data
754 protection assessment as necessary to account for any material change
755 to the processing operations of the online service, product or feature that
756 is the subject of such data protection assessment; and (2) maintain
757 documentation concerning such data protection assessment for the
758 longer of (A) the three-year period beginning on the date on which such
759 processing operations cease, or (B) as long as such controller offers such
760 online service, product or feature.

761 (c) A single data protection assessment may address a comparable set
762 of processing operations that include similar activities.

763 (d) If a controller conducts a data protection assessment for the
764 purpose of complying with another applicable law or regulation, the
765 data protection assessment shall be deemed to satisfy the requirements
766 established in this section if such data protection assessment is
767 reasonably similar in scope and effect to the data protection assessment
768 that would otherwise be conducted pursuant to this section.

769 (e) If any controller conducts a data protection assessment pursuant
770 to subsection (a) of this section and determines that the online service,
771 product or feature that is the subject of such assessment poses a
772 heightened risk of harm to minors, such controller shall establish and
773 implement a plan to mitigate or eliminate such risk.

774 (f) Data protection assessments shall be confidential and shall be
775 exempt from disclosure under the Freedom of Information Act, as
776 defined in section 1-200 of the general statutes. To the extent any
777 information contained in a data protection assessment disclosed to the
778 Attorney General includes information subject to the attorney-client

779 privilege or work product protection, such disclosure shall not
780 constitute a waiver of such privilege or protection.

781 Sec. 11. (NEW) (*Effective October 1, 2024*) (a) A processor shall adhere
782 to the instructions of a controller, and shall: (1) Assist the controller in
783 meeting the controller's obligations under sections 8 to 13, inclusive, of
784 this act taking into account (A) the nature of the processing, (B) the
785 information available to the processor by appropriate technical and
786 organizational measures, and (C) whether such assistance is reasonably
787 practicable and necessary to assist the controller in meeting such
788 obligations; and (2) provide any information that is necessary to enable
789 the controller to conduct and document data protection assessments.

790 (b) A contract between a controller and a processor shall satisfy the
791 requirements established in subsection (b) of section 42-521 of the
792 general statutes.

793 (c) Nothing in this section shall be construed to relieve a controller or
794 processor from the liabilities imposed on the controller or processor by
795 virtue of such controller's or processor's role in the processing
796 relationship, as described in sections 8 to 13, inclusive, of this act.

797 (d) Determining whether a person is acting as a controller or
798 processor with respect to a specific processing of data is a fact-based
799 determination that depends upon the context in which personal data is
800 to be processed. A person who is not limited in such person's processing
801 of personal data pursuant to a controller's instructions, or who fails to
802 adhere to such instructions, is a controller and not a processor with
803 respect to a specific processing of data. A processor that continues to
804 adhere to a controller's instructions with respect to a specific processing
805 of personal data remains a processor. If a processor begins, alone or
806 jointly with others, determining the purposes and means of the
807 processing of personal data, the processor is a controller with respect to
808 such processing and may be subject to an enforcement action under
809 section 13 of this act.

810 Sec. 12. (NEW) (*Effective October 1, 2024*) (a) The provisions of sections

811 8 to 11, inclusive, and section 13 of this act shall not apply to any: (1)
812 Body, authority, board, bureau, commission, district or agency of this
813 state or of any political subdivision of this state; (2) organization that is
814 exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6) or
815 501(c)(12) of the Internal Revenue Code of 1986, or any subsequent
816 corresponding internal revenue code of the United States, as amended
817 from time to time; (3) individual who, or school, board, association,
818 limited liability company or corporation that, is licensed or accredited
819 to offer one or more programs of higher learning leading to one or more
820 degrees; (4) national securities association that is registered under 15
821 USC 78o-3, as amended from time to time; (5) financial institution or
822 data that is subject to Title V of the Gramm-Leach-Bliley Act, 15 USC
823 6801 et seq., as amended from time to time; (6) covered entity or business
824 associate, as defined in 45 CFR 160.103, as amended from time to time;
825 (7) tribal nation government organization; or (8) air carrier, as defined
826 in 49 USC 40102, as amended from time to time, and regulated under
827 the Federal Aviation Act of 1958, 49 USC 40101 et seq., and the Airline
828 Deregulation Act of 1978, 49 USC 41713, as said acts may be amended
829 from time to time.

830 (b) The following information and data is exempt from the provisions
831 of sections 8 to 11, inclusive, and section 13 of this act: (1) Protected
832 health information; (2) patient-identifying information for the purposes
833 of 42 USC 290dd-2, as amended from time to time; (3) identifiable
834 private information for the purposes of the federal policy for the
835 protection of human subjects under 45 CFR 46, as amended from time
836 to time; (4) identifiable private information that is otherwise information
837 collected as part of human subjects research pursuant to the good
838 clinical practice guidelines issued by the International Council for
839 Harmonisation of Technical Requirements for Pharmaceuticals for
840 Human Use, as amended from time to time; (5) the protection of human
841 subjects under 21 CFR Parts 6, 50 and 56, as amended from time to time,
842 or personal data used or shared in research, as defined in 45 CFR
843 164.501, as amended from time to time, that is conducted in accordance
844 with the standards set forth in this subdivision and subdivisions (3) and

845 (4) of this subsection, or other research conducted in accordance with
846 applicable law; (6) information and documents created for the purposes
847 of the Health Care Quality Improvement Act of 1986, 42 USC 11101 et
848 seq., as amended from time to time; (7) patient safety work products for
849 the purposes of section 19a-127o of the general statutes and the Patient
850 Safety and Quality Improvement Act, 42 USC 299b-21 et seq., as
851 amended from time to time; (8) information derived from any of the
852 health care-related information listed in this subsection that is de-
853 identified in accordance with the requirements for de-identification
854 under HIPAA; (9) information originating from and intermingled so as
855 to be indistinguishable from, or information treated in the same manner
856 as, information that is exempt under this subsection and maintained by
857 a covered entity or business associate, program or qualified service
858 organization, as specified in 42 USC 290dd-2, as amended from time to
859 time; (10) information used for public health activities and purposes as
860 authorized by HIPAA, community health activities and population
861 health activities; (11) the collection, maintenance, disclosure, sale,
862 communication or use of any personal information bearing on a
863 consumer's credit worthiness, credit standing, credit capacity, character,
864 general reputation, personal characteristics or mode of living by a
865 consumer reporting agency, furnisher or user that provides information
866 for use in a consumer report, and by a user of a consumer report, but
867 only to the extent that such activity is regulated by and authorized
868 under the Fair Credit Reporting Act, 15 USC 1681 et seq., as amended
869 from time to time; (12) personal data collected, processed, sold or
870 disclosed in compliance with the Driver's Privacy Protection Act of 1994,
871 18 USC 2721 et seq., as amended from time to time; (13) personal data
872 regulated by the Family Educational Rights and Privacy Act, 20 USC
873 1232g et seq., as amended from time to time; (14) personal data collected,
874 processed, sold or disclosed in compliance with the Farm Credit Act, 12
875 USC 2001 et seq., as amended from time to time; (15) data processed or
876 maintained (A) in the course of an individual applying to, employed by
877 or acting as an agent or independent contractor of a controller, processor
878 or third party, to the extent that the data is collected and used within the
879 context of that role, (B) as the emergency contact information of an

880 individual under sections 8 to 11, inclusive, and section 13 of this act
881 used for emergency contact purposes, or (C) that is necessary to retain
882 to administer benefits for another individual relating to the individual
883 who is the subject of the information under subdivision (1) of this
884 subsection and used for the purposes of administering such benefits;
885 and (16) personal data collected, processed, sold or disclosed in relation
886 to price, route or service, as such terms are used in the Federal Aviation
887 Act of 1958, 49 USC 40101 et seq., and the Airline Deregulation Act of
888 1978, 49 USC 41713, as said acts may be amended from time to time.

889 (c) No provision of this section or sections 8 to 11, inclusive, or section
890 13 of this act shall be construed to restrict a controller's or processor's
891 ability to: (1) Comply with federal, state or municipal ordinances or
892 regulations; (2) comply with a civil, criminal or regulatory inquiry,
893 investigation, subpoena or summons by federal, state, municipal or
894 other governmental authorities; (3) cooperate with law enforcement
895 agencies concerning conduct or activity that the controller or processor
896 reasonably and in good faith believes may violate federal, state or
897 municipal ordinances or regulations; (4) investigate, establish, exercise,
898 prepare for or defend legal claims; (5) take immediate steps to protect
899 an interest that is essential for the life or physical safety of the minor or
900 another individual, and where the processing cannot be manifestly
901 based on another legal basis; (6) prevent, detect, protect against or
902 respond to security incidents, identity theft, fraud, harassment,
903 malicious or deceptive activities or any illegal activity, preserve the
904 integrity or security of systems or investigate, report or prosecute those
905 responsible for any such action; (7) engage in public or peer-reviewed
906 scientific or statistical research in the public interest that adheres to all
907 other applicable ethics and privacy laws and is approved, monitored
908 and governed by an institutional review board that determines, or
909 similar independent oversight entities that determine, (A) whether the
910 deletion of the information is likely to provide substantial benefits that
911 do not exclusively accrue to the controller or processor, (B) the expected
912 benefits of the research outweigh the privacy risks, and (C) whether the
913 controller or processor has implemented reasonable safeguards to

914 mitigate privacy risks associated with research, including, but not
915 limited to, any risks associated with re-identification; (8) assist another
916 controller, processor or third party with any obligation under sections 8
917 to 11, inclusive, or section 13 of this act; or (9) process personal data for
918 reasons of public interest in the area of public health, community health
919 or population health, but solely to the extent that such processing is (A)
920 subject to suitable and specific measures to safeguard the rights of the
921 minor whose personal data is being processed, and (B) under the
922 responsibility of a professional subject to confidentiality obligations
923 under federal, state or local law.

924 (d) No obligation imposed on a controller or processor under any
925 provision of sections 8 to 11, inclusive, or section 13 of this act shall be
926 construed to restrict a controller's or processor's ability to collect, use or
927 retain data for internal use to: (1) Conduct internal research to develop,
928 improve or repair products, services or technology; (2) effectuate a
929 product recall; (3) identify and repair technical errors that impair
930 existing or intended functionality; or (4) perform internal operations
931 that are (A) reasonably aligned with the expectations of a minor or
932 reasonably anticipated based on the minor's existing relationship with
933 the controller or processor, or (B) otherwise compatible with processing
934 data in furtherance of the provision of a product or service specifically
935 requested by a minor.

936 (e) No controller or processor shall be required to comply with any
937 provision of sections 8 to 11, inclusive, or section 13 of this act if
938 compliance with such provision would violate an evidentiary privilege
939 under the laws of this state, and no such provision shall be construed to
940 prevent a controller or processor from providing, as part of a privileged
941 communication, any personal data concerning a minor to any other
942 person who is covered by such evidentiary privilege.

943 (f) No provision of sections 8 to 11, inclusive, or section 13 of this act
944 shall be construed to: (1) Impose any obligation on a controller that
945 adversely affects the rights or freedoms of any person, including, but
946 not limited to, the rights of any person (A) to freedom of speech or

947 freedom of the press guaranteed in the First Amendment to the United
948 States Constitution, or (B) under section 52-146t of the general statutes;
949 or (2) apply to any individual's processing of personal data in the course
950 of such individual's purely personal or household activities.

951 (g) (1) Any personal data processed by a controller pursuant to this
952 section may be processed to the extent that such processing is: (A)
953 Reasonably necessary and proportionate to the purposes listed in this
954 section; and (B) adequate, relevant and limited to what is necessary in
955 relation to the specific purposes listed in this section.

956 (2) Any controller that collects, uses or retains data pursuant to
957 subsection (d) of this section shall, where applicable, take into account
958 the nature and purpose or purposes of such collection, use or retention.
959 Such data shall be subject to reasonable administrative, technical and
960 physical measures to protect the confidentiality, integrity and
961 accessibility of the personal data and to reduce reasonably foreseeable
962 risks of harm to minors concerning such collection, use or retention of
963 personal data.

964 (h) If any controller or processor processes personal data pursuant to
965 an exemption established in subsections (a) to (g), inclusive, of this
966 section, such controller or processor bears the burden of demonstrating
967 that such processing qualifies for such exemption and complies with the
968 requirements established in subsection (g) of this section.

969 Sec. 13. (NEW) (*Effective October 1, 2024*) (a) Any violation of the
970 provisions of sections 8 to 12, inclusive, of this act shall constitute an
971 unfair trade practice under subsection (a) of section 42-110b of the
972 general statutes and shall be enforced solely by the Attorney General.
973 Nothing in this section or sections 8 to 12, inclusive, of this act shall be
974 construed to create a private right of action or to provide grounds for an
975 action under section 42-110g of the general statutes.

976 (b) (1) During the period beginning October 1, 2024, and ending
977 December 31, 2025, if the Attorney General, in the Attorney General's
978 discretion, determines that a controller or processor has violated any

979 provision of sections 8 to 12, inclusive, of this act but may cure such
980 alleged violation, the Attorney General shall provide written notice to
981 such controller or processor, in a form and manner prescribed by the
982 Attorney General and before the Attorney General commences any
983 action to enforce such provision, disclosing such alleged violation and
984 such provision.

985 (2) (A) Not later than thirty days after a controller or processor
986 receives a notice under subdivision (1) of this subsection, the controller
987 or processor may send a notice to the Attorney General, in a form and
988 manner prescribed by the Attorney General, disclosing that such
989 controller or processor has: (i) Determined that such controller or
990 processor did not commit the alleged violation of sections 8 to 12,
991 inclusive, of this act; or (ii) cured such violation and taken measures that
992 are sufficient to prevent further such violations.

993 (B) If the Attorney General receives a notice described in
994 subparagraph (A) of this subdivision and determines, in the Attorney
995 General's discretion, that the controller or processor that sent such
996 notice did not commit the alleged violation or has cured such violation
997 and taken the measures described in subparagraph (A)(ii) of this
998 subdivision, such controller or processor shall not be liable for any civil
999 penalty under subsection (a) of this section.

1000 (C) Not later than February 1, 2026, the Attorney General shall submit
1001 a report, in accordance with section 11-4a of the general statutes, to the
1002 joint standing committee of the General Assembly having cognizance of
1003 matters relating to general law. Such report shall disclose: (i) The
1004 number of notices the Attorney General has issued pursuant to
1005 subdivision (1) of this subsection; (ii) the number of violations that were
1006 cured pursuant to subparagraphs (A) and (B) of this subdivision; and
1007 (iii) any other matter the Attorney General deems relevant for the
1008 purposes of such report.

1009 (c) Beginning on January 1, 2026, the Attorney General may, in the
1010 Attorney General's discretion, provide to a controller or processor an

1011 opportunity to cure any alleged violation of the provisions of sections 8
1012 to 12, inclusive, of this act in the manner described in subdivisions (1)
1013 and (2) of subsection (b) of this section. In determining whether to grant
1014 the controller or processor an opportunity to cure such alleged violation,
1015 the Attorney General may consider: (1) The number of such violations
1016 that such controller or processor is alleged to have committed; (2) the
1017 size and complexity of such controller or processor; (3) the nature and
1018 extent of such controller's or processor's processing activities; (4)
1019 whether there exists a substantial likelihood that such alleged violation
1020 has caused or will cause public injury; (5) the safety of persons or
1021 property; (6) whether such alleged violation was likely caused by a
1022 human or technical error; and (7) the sensitivity of the data.

1023 Sec. 14. Section 21a-435 of the general statutes is repealed and the
1024 following is substituted in lieu thereof (*Effective January 1, 2024*):

1025 As used in this section, [and] sections 21a-436 to 21a-439, inclusive, as
1026 amended by this act, and section 15 of this act:

1027 (1) "Connecticut user" means a user who provides a Connecticut
1028 home address or zip code when registering with an online dating
1029 operator or a user who is known or determined by an online dating
1030 operator or its online dating platform to be in Connecticut at the time of
1031 registration;

1032 (2) "Criminal background screening" means a name search for an
1033 individual's history of criminal convictions that is conducted by
1034 searching an (A) available and regularly updated government public
1035 record database that in the aggregate provides national coverage for
1036 searching an individual's history of criminal convictions; or (B) a
1037 regularly updated database maintained by a private vendor that
1038 provides national coverage for searching an individual's history of
1039 criminal convictions and sexual offender registries;

1040 (3) "Criminal conviction" means a conviction for a crime in this state,
1041 another state, or under federal law;

1042 (4) "Online dating" means the act of using a digital service to initiate
1043 relationships with other individuals for the purpose of romance, sex or
1044 marriage;

1045 (5) "Online dating operator" means a person who operates a software
1046 application designed to facilitate online dating;

1047 (6) "Online dating platform" means a digital service designed to allow
1048 users to interact through the Internet to participate in online dating; and

1049 (7) "User" means an individual who uses the online dating services of
1050 an online dating operator.

1051 Sec. 15. (NEW) (*Effective January 1, 2024*) (a) Each online dating
1052 operator that offers services to Connecticut users shall maintain an
1053 online safety center, which shall be reasonably designed to provide
1054 Connecticut users with resources concerning safe dating. Each online
1055 safety center maintained pursuant to this subsection shall provide: (1)
1056 An explanation of the online dating operator's reporting mechanism for
1057 harmful or unwanted behavior; (2) safety advice for use when
1058 communicating online and meeting in person; (3) a link to an Internet
1059 web site or a telephone number where a Connecticut user may access
1060 resources concerning domestic violence and sexual harassment; and (4)
1061 educational information concerning romance scams.

1062 (b) Each online dating operator that offers services to Connecticut
1063 users shall adopt a policy for the online dating platform's handling of
1064 harassment reports by or between users.

1065 Sec. 16. Section 21a-439 of the general statutes is repealed and the
1066 following is substituted in lieu thereof (*Effective January 1, 2024*):

1067 (a) The Department of Consumer Protection may issue fines of not
1068 more than twenty-five thousand dollars per violation, accept an offer in
1069 compromise, or take other actions permitted by the general statutes or
1070 the regulations of Connecticut state agencies if an online dating operator
1071 fails to comply with the provisions of sections 21a-435 to 21a-438,

1072 inclusive, as amended by this act, and section 15 of this act.

1073 (b) The Commissioner of Consumer Protection, or the commissioner's
1074 designee, may conduct investigations and hold hearings on any matter
1075 under the provisions of this section, [and] sections 21a-435 to 21a-438,
1076 inclusive, as amended by this act, and section 15 of this act. The
1077 commissioner, or the commissioner's designee, may issue subpoenas,
1078 administer oaths, compel testimony and order the production of books,
1079 records and documents. If any person refuses to appear, to testify or to
1080 produce any book, record or document when so ordered, upon
1081 application of the commissioner or the commissioner's designee, a judge
1082 of the Superior Court may make such order as may be appropriate to
1083 aid in the enforcement of this section.

1084 (c) The Attorney General, at the request of the commissioner or the
1085 commissioner's designee, may apply in the name of the state to the
1086 Superior Court for an order temporarily or permanently restraining and
1087 enjoining any person from violating any provision of this section, [and]
1088 sections 21a-435 to 21a-438, inclusive, as amended by this act, and
1089 section 15 of this act.

1090 Sec. 17. Section 29-7b of the general statutes is repealed and the
1091 following is substituted in lieu thereof (*Effective July 1, 2023*):

1092 (a) There shall be within the Department of Emergency Services and
1093 Public Protection a Division of Scientific Services. The Commissioner of
1094 Emergency Services and Public Protection shall serve as administrative
1095 head of such division, and may delegate jurisdiction over the affairs of
1096 such division to a deputy commissioner.

1097 (b) The Division of Scientific Services shall provide technical
1098 assistance to law enforcement agencies in the various areas of scientific
1099 investigation. The division shall maintain facilities and services for the
1100 examination and analysis of evidentiary materials in areas including,
1101 but not limited to, chemistry, arson, firearms, questioned documents,
1102 microscopy, serology, toxicology, trace evidence, latent fingerprints,
1103 impressions and other similar technology. The facilities, services and

1104 personnel of the division shall be available, without charge, to the Office
1105 of the Chief Medical Examiner and all duly constituted prosecuting,
1106 police and investigating agencies of the state.

1107 (c) The Division of Scientific Services: (1) May investigate any
1108 physical evidence or evidentiary material related to a crime upon the
1109 request of any federal, state or local agency, (2) may conduct or assist in
1110 the scientific field investigation at the scene of a crime and provide other
1111 technical assistance and training in the various fields of scientific
1112 criminal investigation upon request, (3) shall assure the safe custody of
1113 evidence during examination, (4) shall forward a written report of the
1114 results of an examination of evidence to the agency submitting such
1115 evidence, (5) shall render expert court testimony when requested, and
1116 (6) shall conduct ongoing research in the areas of the forensic sciences.
1117 The Commissioner of Emergency Services and Public Protection or a
1118 director designated by the commissioner shall be in charge of the
1119 Division of Scientific Services operations and shall establish and
1120 maintain a system of case priorities and a procedure for submission of
1121 evidence and evidentiary security. The director of the Division of
1122 Scientific Services shall be in the unclassified service and shall serve at
1123 the pleasure of the commissioner.

1124 (d) In accordance with the provisions of sections 4-38d, 4-38e and 4-
1125 39, all powers and duties of the Department of Public Health under the
1126 provisions of sections 14-227a, 14-227c, 15-140u and 21a-283 shall be
1127 transferred to the Division of Scientific Services within the Department
1128 of Emergency Services and Public Protection.

1129 (e) There is established within the Division of Scientific Services the
1130 Connecticut Internet Crimes Against Children Task Force, which shall
1131 consist of affiliate law enforcement agencies in the state. The task force
1132 shall use state and federal moneys appropriated to it in a manner that is
1133 consistent with the duties prescribed in 34 USC 21114."

This act shall take effect as follows and shall amend the following sections:

| | | |
|-----------|------------------------|------------------|
| Section 1 | <i>July 1, 2023</i> | 42-515 |
| Sec. 2 | <i>July 1, 2023</i> | New section |
| Sec. 3 | <i>July 1, 2023</i> | 42-517(a) to (c) |
| Sec. 4 | <i>July 1, 2023</i> | 42-520(a) |
| Sec. 5 | <i>July 1, 2023</i> | 42-524 |
| Sec. 6 | <i>July 1, 2023</i> | 42-525 |
| Sec. 7 | <i>July 1, 2024</i> | New section |
| Sec. 8 | <i>October 1, 2024</i> | New section |
| Sec. 9 | <i>October 1, 2024</i> | New section |
| Sec. 10 | <i>October 1, 2024</i> | New section |
| Sec. 11 | <i>October 1, 2024</i> | New section |
| Sec. 12 | <i>October 1, 2024</i> | New section |
| Sec. 13 | <i>October 1, 2024</i> | New section |
| Sec. 14 | <i>January 1, 2024</i> | 21a-435 |
| Sec. 15 | <i>January 1, 2024</i> | New section |
| Sec. 16 | <i>January 1, 2024</i> | 21a-439 |
| Sec. 17 | <i>July 1, 2023</i> | 29-7b |