

1 S.71

2 An act relating to consumer data privacy and online surveillance

3 The House proposes to the Senate to amend the bill by striking out all after
4 the enacting clause and inserting in lieu thereof the following:

5 Sec. 1. 9 V.S.A. chapter 61A is added to read:

6 CHAPTER 61A. DATA PRIVACY

7 Subchapter 1. Vermont Data Privacy and Online Surveillance Act

8 § 2415a. SHORT TITLE AND DEFINITIONS

9 (a) Short title. This subchapter shall be known and may be cited as the
10 “Vermont Data Privacy and Online Surveillance Act.”

11 (b) Definitions. As used in this subchapter:

12 (1)(A) “Affiliate” means a legal entity that shares common branding
13 with another legal entity or controls, is controlled by, or is under common
14 control with another legal entity.

15 (B) As used in subdivision (A) of this subdivision (1), “control” or
16 “controlled” means:

17 (i) ownership of, or the power to vote, more than 50 percent of the
18 outstanding shares of any class of voting security of a company;

19 (ii) control in any manner over the election of a majority of the
20 directors or of individuals exercising similar functions; or

1 (iii) the power to exercise controlling influence over the
2 management of a company.

3 (2) “Authenticate” means to use reasonable means to determine that a
4 request to exercise any of the rights afforded under subdivisions 2415d(a)(1)–
5 (4) of this subchapter is being made by, or on behalf of, the consumer who is
6 entitled to exercise the consumer rights with respect to the personal data at
7 issue.

8 (3)(A) “Biometric data” means data generated from the technological
9 processing of an individual’s unique biological, physical, or physiological
10 characteristics that are collected on or used to identify a specific consumer,
11 including:

12 (i) iris or retina scans;

13 (ii) fingerprints;

14 (iii) facial or hand mapping, geometry, or templates;

15 (iv) vein patterns;

16 (v) voice prints or vocal biomarkers; and

17 (vi) gait or personally identifying physical movement or patterns.

18 (B) “Biometric data” does not include:

19 (i) a digital or physical photograph;

20 (ii) an audio or video recording; or

1 (iii) any data generated from a digital or physical photograph or an
2 audio or video recording, unless such data is generated to identify a specific
3 individual.

4 (4) “Business associate” has the same meaning as in HIPAA.

5 (5) “Child” has the same meaning as in COPPA.

6 (6)(A) “Collect,” “collected,” or “collection” means buying, renting,
7 gathering, obtaining, receiving, or accessing any personal data by any means,
8 other than such activities between a controller and a processor or between a
9 processor and its subcontractors.

10 (B) “Collect,” “collected,” or “collection” includes receiving data
11 from the consumer, either actively or passively, or by observing the
12 consumer’s behavior.

13 (7)(A) “Consent” means a clear affirmative act signifying a consumer’s
14 freely given, specific, informed, and unambiguous agreement to allow the
15 processing of personal data relating to the consumer.

16 (B) “Consent” may include a written statement, including by
17 electronic means, or any other unambiguous affirmative action.

18 (C) “Consent” does not include:

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

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

3 (iii) agreement obtained through the use of dark patterns.

4 (8)(A) “Consumer” means an individual who is a resident of the State.

5 (B) “Consumer” does not include an individual acting in a
6 commercial or employment context or as an employee, owner, director, officer,
7 or contractor of a company, partnership, sole proprietorship, nonprofit
8 organization, or government agency whose communications or transactions
9 with the controller occur solely within the context of that individual’s role with
10 the company, partnership, sole proprietorship, nonprofit organization, or
11 government agency.

12 (9) “Consumer health data” means any personal data that a controller
13 uses to identify a consumer’s physical or mental health condition, diagnosis, or
14 status, including gender-affirming health data and reproductive or sexual
15 health data.

16 (10) “Consumer health data controller” means any controller that, alone
17 or jointly with others, determines the purpose and means of processing
18 consumer health data.

19 (11) “Consumer reporting agency” has the same meaning as in the Fair
20 Credit Reporting Act, 15 U.S.C. § 1681a(f).

1 (12) “Controller” means a person who, alone or jointly with others,
2 determines the purpose and means of processing personal data.

3 (13) “COPPA” means the Children’s Online Privacy Protection Act of
4 1998, 15 U.S.C. §§ 6501–6506, and any regulations, rules, guidance, and
5 exemptions adopted pursuant to the act, as the act and regulations, rules,
6 guidance, and exemptions may be amended.

7 (14) “Covered entity” has the same meaning as in HIPAA.

8 (15) “Credit union” has the same meaning as in 8 V.S.A. § 30101.

9 (16) “Dark pattern” means a user interface designed or manipulated with
10 the substantial effect of subverting or impairing user autonomy, decision
11 making, or choice and includes any practice the Federal Trade Commission
12 refers to as a “dark pattern.”

13 (17) “Decision that produces any legal or similarly significant effect”
14 means any decision made by the controller, or on behalf of the controller, that
15 results in the provision or denial by the controller of any financial or lending
16 service, any housing, any insurance, any education enrollment or opportunity,
17 any criminal justice, any employment opportunity, or any health care service.

18 (18) “Deidentified data” means data that does not identify and cannot
19 reasonably be used to infer information about, or otherwise be linked to, an
20 identified or identifiable individual, or a device linked to the individual, if the
21 controller that possesses the data:

1 (A)(i) takes reasonable measures to ensure that the data cannot be
2 used to reidentify an identified or identifiable individual or be associated with
3 an individual or device that identifies or is linked or reasonably linkable to an
4 individual; and

5 (ii) for purposes of this subdivision (A), “reasonable measures”
6 includes the deidentification requirements set forth under 45 C.F.R § 164.514
7 (other requirements relating to uses and disclosures of protected health
8 information);

9 (B) publicly commits to process the data only in a deidentified
10 fashion and not attempt to reidentify the data; and

11 (C) contractually obligates any recipients of the data to comply with
12 all provisions of this subchapter.

13 (19) “Derived data” means data that is created by the derivation of
14 information, data, assumptions, correlations, inferences, predictions, or
15 conclusions from facts, evidence, or another source of information or data
16 about a consumer’s device.

17 (20) “Gender-affirming health care services” has the same meaning as in
18 1 V.S.A. § 150.

19 (21) “Gender-affirming health data” means any personal data
20 concerning a past, present, or future effort made by a consumer to seek, or a
21 consumer’s receipt of, gender-affirming health care services.

1 (22) “Genetic data” means any data, regardless of its format, that results
2 from the analysis of a biological sample of an individual, or from another
3 source enabling equivalent information to be obtained, and concerns genetic
4 material, including deoxyribonucleic acids (DNA), ribonucleic acids (RNA),
5 genes, chromosomes, alleles, genomes, alterations or modifications to DNA or
6 RNA, single nucleotide polymorphisms (SNPs), epigenetic markers,
7 uninterpreted data that results from analysis of the biological sample or other
8 source, and any information extrapolated, derived, or inferred therefrom.

9 (23) “Geofence” means any technology that uses global positioning
10 coordinates, cell tower connectivity, cellular data, radio frequency
11 identification, wireless fidelity technology data, or any other form of location
12 detection, or any combination of such coordinates, connectivity, data,
13 identification, or other form of location detection, to establish a virtual
14 boundary.

15 (24) “Health care facility” has the same meaning as in 18 V.S.A. § 9432.

16 (25) “HIPAA” means the Health Insurance Portability and
17 Accountability Act of 1996, Pub. L. No. 104-191, as may be amended.

18 (26) “Hybrid entity” has the same meaning as in HIPAA.

19 (27) “Identified or identifiable individual” means an individual who can
20 be readily identified, directly or indirectly, including by reference to an

1 identifier such as a name, an identification number, precise geolocation data, or
2 an online identifier.

3 (28) “Institution of higher education” means any individual who, or
4 school, board, association, limited liability company, or corporation that, is
5 licensed or accredited to offer one or more programs of higher learning leading
6 to one or more degrees.

7 (29) “Mental health facility” means any health care facility in which at
8 least 70 percent of the health care services provided in the facility are mental
9 health services.

10 (30) “Minor” means any consumer who is younger than 18 years of age.

11 (31) “Neural data” means any information that is generated by
12 measuring the activity of an individual’s central nervous system.

13 (32) “Nonprofit organization” means any organization that is qualified
14 for tax exempt status under I.R.C. § 501(c)(3), 501(c)(4), 501(c)(6), or
15 501(c)(12), or any corresponding internal revenue code of the United States, as
16 may be amended.

17 (33) “Patient-identifying information” has the same meaning as in
18 42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).

19 (34) “Person” means an individual, association, company, limited
20 liability company, corporation, partnership, sole proprietorship, trust, or other
21 legal entity.

1 (35)(A) “Personal data” means any information, including derived data
2 and unique identifiers, that is linked or reasonably linkable, alone or in
3 combination with other information, to an identified or identifiable individual
4 or to a device that identifies, is linked to, or is reasonably linkable to one or
5 more identified or identifiable individuals.

6 (B) “Personal data” does not include deidentified data or publicly
7 available information.

8 (36)(A) “Precise geolocation data” means information derived from
9 technology, including global positioning system level latitude and longitude
10 coordinates or other mechanisms, that directly identifies the specific location
11 of an individual with precision and accuracy within a radius of 1,750 feet.

12 (B) “Precise geolocation data” does not include:

13 (i) the content of communications;

14 (ii) data generated by or connected to an advanced utility metering
15 infrastructure system; or

16 (iii) data generated by equipment used by a utility company.

17 (37) “Process” or “processing” means any operation or set of operations
18 performed, whether by manual or automated means, on personal data or on sets
19 of personal data, such as the collection, use, storage, disclosure, analysis,
20 deletion, or modification of personal data.

1 (38) “Processor” means a person who collects or processes personal data
2 on behalf of:

3 (A) a controller; or

4 (B) another processor.

5 (39) “Profiling” means any form of automated processing performed on
6 personal data to evaluate, analyze, or predict personal aspects, including an
7 individual’s economic situation, health, personal preferences, interests,
8 reliability, behavior, location, movements, or identifying characteristics.

9 (40) “Protected health information” has the same meaning as in HIPAA.

10 (41) “Pseudonymous data” means personal data that cannot be attributed
11 to a specific individual without the use of additional information, provided the
12 additional information is kept separately and is subject to appropriate technical
13 and organizational measures to ensure that the personal data are not attributed
14 to an identified or identifiable individual.

15 (42)(A) “Publicly available information” means information that:

16 (i) is made available through federal, state, or local government
17 records or to the general public from widely distributed media; or

18 (ii) a controller has a reasonable basis to believe that the consumer
19 has lawfully made available to the general public.

- 1 (B) “Publicly available information” does not include:
- 2 (i) biometric data collected by a business about a consumer
3 without the consumer’s knowledge;
- 4 (ii) information that is collated and combined to create a consumer
5 profile that is made available to a user of a publicly available website either in
6 exchange for payment or free of charge;
- 7 (iii) an inference that is generated from the information described
8 in subdivision (ii) of this subdivision (42)(B);
- 9 (iv) solely for the purposes set forth in subdivisions 2415d(a)(1),
10 (2), and (4) of this subchapter, information that is made available for sale;
- 11 (v) any obscene visual depiction, as defined in 18 U.S.C. § 1460;
- 12 (vi) personal data that is created through the combination of
13 personal data with publicly available information;
- 14 (vii) genetic data, unless otherwise made publicly available by the
15 consumer to whom the information pertains;
- 16 (viii) information provided by a consumer on a website or online
17 service made available to all members of the public, for free or for a fee, where
18 the consumer has maintained a reasonable expectation of privacy in the
19 information, such as by restricting the information to a specific audience; or
- 20 (ix) intimate images, authentic or computer generated, known to
21 be nonconsensual.

1 (43) “Reproductive or sexual health care” has the same meaning as
2 “reproductive health care services” in 1 V.S.A. § 150(c).

3 (44) “Reproductive or sexual health data” means any personal data
4 concerning an effort made by a consumer to seek, or a consumer’s receipt of,
5 reproductive or sexual health care.

6 (45) “Reproductive or sexual health facility” means any health care
7 facility in which at least 70 percent of the health care–related services or
8 products rendered or provided in the facility are reproductive or sexual health
9 care.

10 (46)(A) “Sale of personal data” means the exchange of a consumer’s
11 personal data by the controller with a third party for monetary or other valuable
12 consideration.

13 (B) “Sale of personal data” does not include:

14 (i) the disclosure of personal data to a processor that processes the
15 personal data on behalf of the controller;

16 (ii) the disclosure of personal data to a third party for purposes of
17 providing a product or service requested by the consumer;

18 (iii) the disclosure or transfer of personal data to an affiliate of the
19 controller;

1 (iv) the disclosure of personal data when the consumer directs the
2 controller to disclose the personal data or intentionally uses the controller to
3 interact with a third party;

4 (v) the disclosure of personal data that the consumer:

5 (I) intentionally made available to the general public via a
6 channel of mass media; and

7 (II) did not restrict to a specific audience; or

8 (vi) the disclosure or transfer of personal data to a third party as an
9 asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a
10 proposed merger, acquisition, bankruptcy, or other transaction, in which the
11 third party assumes control of all or part of the controller’s assets.

12 (47) “Sensitive data” means personal data that includes:

13 (A) data revealing:

14 (i) racial or ethnic origin, religious beliefs, sex life, sexual
15 orientation, status as nonbinary or transgender, or citizenship or immigration

16 status; or

17 (ii) a mental or physical health condition, diagnosis, disability, or
18 treatment;

19 (B) consumer health data;

20 (C) genetic or biometric data or information derived therefrom;

1 (D) personal data collected from an individual the controller has
2 actual knowledge, or willfully disregards, is a child;

3 (E) precise geolocation data;

4 (F) neural data;

5 (G) a consumer’s financial account number, financial account login
6 information, or credit card or debit card number that, in combination with any
7 required access or security code, password, or credential, would allow access
8 to a consumer’s financial account; or

9 (H) a government-issued identification number, including, but not
10 limited to, Social Security number, passport number, State identification card
11 number, or driver’s license number, that applicable law does not require to be
12 publicly displayed.

13 (48)(A) “Targeted advertising” means displaying advertisements to a
14 consumer where the advertisement is selected based on personal data obtained
15 or inferred from that consumer’s activities over time and across nonaffiliated
16 websites or online applications to predict the consumer’s preferences or
17 interests.

18 (B) “Targeted advertising” does not include:

19 (i) an advertisement based on activities within the controller’s own
20 website or online application;

1 (ii) an advertisement based on the context of a consumer’s current
2 search query or visit to a website or online application;

3 (iii) an advertisement directed to a consumer in response to the
4 consumer’s request for information or feedback; or

5 (iv) processing of personal data solely to measure or report
6 advertising frequency, performance, or reach.

7 (49) “Third party” means a person, public authority, agency, or body,
8 other than the consumer, controller, or processor or an affiliate of the processor
9 or the controller.

10 (50) “Trade secret” has the same meaning as in section 4601 of this title.

11 § 2415b. APPLICABILITY

12 (a) Thresholds. Except as provided in subsection (b) of this section, this
13 subchapter applies to a person that conducts business in this State or a person
14 that produces products or services that are targeted to residents of this State
15 and that during the preceding calendar year:

16 (1) controlled or processed the personal data of not fewer than 35,000
17 consumers, excluding personal data controlled or processed solely for the
18 purpose of completing a payment transaction;

19 (2) controlled or processed the sensitive data of not fewer than 3,000
20 consumers, excluding personal data controlled or processed solely for the
21 purposes of completing a payment transaction; or

1 (3) offered for sale in trade or commerce the personal data of not fewer
2 than 3,000 consumers.

3 (b) Health data applicability. Section 2415k of this subchapter and the
4 provisions of this subchapter concerning consumer health data and consumer
5 health data controllers apply to a person that conducts business in this State or
6 a person that produces products or services that are targeted to residents of this
7 State.

8 (c) Controlling law. In the event of a conflict between the provisions of
9 this subchapter and any other law, including the Vermont Age-Appropriate
10 Design Code Act, the provisions of the law that afford the greatest protection
11 for the right of privacy for consumers shall control.

12 § 2415c. EXEMPTIONS

13 (a) This subchapter does not apply to:

14 (1) in the ordinary course of its operation, a federal, state, tribal, or local
15 government entity or an instrumentality of the State;

16 (2)(A) a covered entity that is not a hybrid entity;

17 (B) any health care component of a hybrid entity; or

18 (C) a business associate;

19 (3) patient-identifying information, for purposes of 42 U.S.C. § 290DD–

20 2;

1 (4)(A) information to the extent it is used for public health, community
2 health, or population health activities and purposes, as authorized by HIPAA,
3 when provided by or to a covered entity or when provided by or to a business
4 associate in accordance with the business associate agreement with a covered
5 entity;

6 (B) information that is a health care record, as that term is defined in
7 18 V.S.A. § 9419, if the information is held by an entity that is a covered entity
8 or business associate under HIPAA because it collects, uses, or discloses
9 protected health information;

10 (C) information that is deidentified in accordance with the
11 requirements for deidentification set forth in 45 C.F.R. § 164.514 and that is
12 derived from individually identifiable health information as described in
13 HIPAA; and

14 (D) personal information consistent with the human subject
15 protection requirements of the U.S. Food and Drug Administration;

16 (5) information used only for public health activities and purposes
17 described in 45 C.F.R. § 164.512 (disclosure of protected health information
18 without authorization);

1 (6) information that identifies a consumer in connection with:

2 (A) activities that are subject to the Federal Policy for the Protection
3 of Human Subjects, codified as 45 C.F.R. Part 46 (HHS protection of human
4 subjects) and in various other federal regulations;

5 (B) activities that are subject to the protections provided in 21 C.F.R.
6 Parts 50 (FDA clinical investigations protection of human subjects) and
7 56 (FDA clinical investigations institutional review boards); or

8 (C) research conducted in accordance with the requirements set forth
9 in subdivisions (A) and (B) of this subdivision (a)(6) or otherwise in
10 accordance with applicable law;

11 (7) patient-identifying information that is collected and processed in
12 accordance with 42 C.F.R. Part 2 (confidentiality of substance use disorder
13 patient records);

14 (8) patient safety work product that is created and used for purposes of
15 patient safety improvement in accordance with 42 C.F.R. § 3, established in
16 accordance with 42 U.S.C. §§ 299b–21 through 299b–26;

17 (9) information or documents created for the purposes of the Healthcare
18 Quality Improvement Act of 1986, 42 U.S.C. §§ 11101–11152, and regulations
19 adopted to implement that act;

1 (10) information processed or maintained solely in connection with, and
2 for the purpose of, enabling notice of an emergency to persons that an
3 individual specifies;

4 (11) any activity that involves collecting, maintaining, disclosing,
5 selling, communicating, or using information for the purpose of evaluating a
6 consumer’s creditworthiness, credit standing, credit capacity, character,
7 general reputation, personal characteristics, or mode of living if done strictly in
8 accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C.
9 §§ 1681–1681x, as may be amended, by:

10 (A) a consumer reporting agency;

11 (B) a person who furnishes information to a consumer reporting
12 agency under 15 U.S.C. § 1681s-2 (responsibilities of furnishers of
13 information to consumer reporting agencies); or

14 (C) a person who uses a consumer report as provided in 15 U.S.C.
15 § 1681b(a)(3) (permissible purposes of consumer reports);

16 (12) information collected, processed, sold, or disclosed under and in
17 accordance with the following laws and regulations:

18 (A) the Driver’s Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–
19 2725;

20 (B) data that is subject to the Family Educational Rights and Privacy
21 Act, 20 U.S.C. § 1232g, and regulations adopted to implement that act;

1 (C) data that is subject to the Airline Deregulation Act, Pub. L. No.
2 95-504, only to the extent that an air carrier collects information related to
3 prices, routes, or services, and only to the extent that the provisions of the
4 Airline Deregulation Act preempt this subchapter;

5 (D) data that is subject to the Farm Credit Act, Pub. L. No. 92-181, as
6 may be amended; and

7 (E) data that is subject to federal policy under 21 U.S.C. § 830
8 (regulation of listed chemicals and certain machines);

9 (13) data subject to Title V of the Gramm-Leach-Bliley Act, Pub. L. No.
10 106-102, and regulations adopted to implement that act;

11 (14) a state- or federally chartered bank or credit union, or an affiliate or
12 subsidiary that is principally engaged in financial activities, as described in
13 12 U.S.C. § 1843(k);

14 (15) an agent, broker-dealer, investment adviser, or investment adviser
15 representative, as those terms are defined in section 5102 of this title, who is
16 regulated by the Department of Financial Regulation or the Securities and
17 Exchange Commission;

18 (16) a person regulated pursuant to 8 V.S.A. part 3 (chapters 101–165)
19 other than a person who, alone or in combination with another person,
20 establishes and maintains a self-insurance program and who does not otherwise
21 engage in the business of entering into policies of insurance;

1 (17) health care providers and health care facilities, as those terms are
2 defined in 18 V.S.A. § 9402, provided such providers and facilities maintain
3 all protected health information in accordance with the requirements of
4 18 V.S.A. § 1881 and HIPAA regardless of whether such providers or facilities
5 are covered entities under 45 C.F.R. § 160.103;

6 (18) protected health information under HIPAA;

7 (19) a third-party administrator, as that term is defined in the Third Party
8 Administrator Rule adopted pursuant to 18 V.S.A. § 9417, provided that the
9 third-party administrator is subject to and in compliance with the Department
10 of Financial Regulation’s Regulation IH-2001-01 (Privacy of Consumer
11 Financial and Health Information);

12 (20) personal data of a victim or witness of child abuse, domestic
13 violence, human trafficking, sexual assault, violent felony, or stalking that a
14 victim services organization collects, processes, or maintains in the course of
15 its operation;

16 (21) a nonprofit organization that is established to detect and prevent
17 fraudulent acts in connection with insurance;

18 (22) information that is processed for purposes of compliance,
19 enrollment or degree verification, or research services by a nonprofit
20 organization that is established to provide enrollment data reporting services
21 on behalf of postsecondary schools as that term is defined in 16 V.S.A. § 176;

1 (23) noncommercial activity of:

2 (A) a publisher, editor, reporter, or other person who is connected
3 with or employed by a newspaper, magazine, periodical, newsletter, pamphlet,
4 report, or other publication in general circulation;

5 (B) a radio or television station that holds a license issued by the
6 Federal Communications Commission;

7 (C) a nonprofit organization that provides programming to radio or
8 television networks; or

9 (D) a press association or wire service; or

10 (24) data processed or maintained:

11 (A) in the course of an individual applying to, employed by, or acting
12 as an agent or independent contractor of a controller, processor, consumer
13 health data controller, or third party, to the extent that the data is collected and
14 used within the context of that role;

15 (B) as the emergency contact information of a consumer pursuant to
16 this subchapter, used for emergency contact purposes; or

17 (C) that is necessary to retain to administer benefits for another
18 individual relating to the individual who is the subject of the information
19 pursuant to subdivision (18) of this subsection (a) and used for the purposes of
20 administering such benefits.

1 (b) Controllers, processors, and consumer health data controllers that
2 comply with the verifiable parental consent requirements of COPPA shall be
3 deemed compliant with any obligation to obtain parental consent pursuant to
4 this subchapter.

5 § 2415d. CONSUMER PERSONAL DATA RIGHTS

6 (a) Consumer rights. A consumer shall have the right to:

7 (1) confirm whether or not a controller is processing the consumer's
8 personal data and access such personal data, including any inferences about the
9 consumer derived from such personal data and whether a controller or
10 processor is processing a consumer's personal data for the purposes of
11 profiling to make a decision that produces any legal or similarly significant
12 effect concerning a consumer, unless such confirmation or access would
13 require the controller to reveal a trade secret or the controller is prohibited
14 from disclosing such personal data under subsection (e) of this section;

15 (2) correct inaccuracies in the consumer's personal data, taking into
16 account the nature of the personal data and the purposes of the processing of
17 the consumer's personal data;

18 (3) delete personal data provided by, or obtained about, the consumer;

19 (4) obtain a copy of the consumer's personal data processed by the
20 controller, in a portable and, to the extent technically feasible, readily usable
21 format that allows the consumer to transmit the data to another controller

1 without hindrance, where the processing is carried out by automated means,
2 provided the controller shall not be required to reveal any trade secret;

3 (5) opt out of the processing of the personal data for purposes of:

4 (A) targeted advertising;

5 (B) the sale of personal data, except as provided in subsection
6 2415e(b) of this subchapter; or

7 (C) profiling in furtherance of any automated decision that produces
8 any legal or similarly significant effect concerning the consumer;

9 (6) if the consumer's personal data were processed for the purposes of
10 profiling in furtherance of any automated decision that produced any legal or
11 similarly significant effect concerning the consumer, and if feasible:

12 (A) question the result of such profiling;

13 (B) be informed of the reason that such profiling resulted in such
14 decision;

15 (C) review the consumer's personal data that were processed for the
16 purposes of such profiling; and

17 (D) if the profiling decision concerned housing, taking into account
18 the nature of the personal data and the purposes for which such personal data
19 were processed, be allowed to correct any incorrect personal data that were
20 processed for the purposes of such profiling and have the profiling decision
21 reevaluated based on the corrected personal data; and

1 (7) obtain from the controller a list of the third parties to which such
2 controller has sold the consumer's personal data or, if such controller does not
3 maintain a list of the third parties to which such controller has sold the
4 consumer's personal data, a list of all third parties to which such controller has
5 sold personal data, provided the controller shall not be required to reveal any
6 trade secret.

7 (b) Exercising consumer rights.

8 (1) A consumer may exercise rights under this section by a secure and
9 reliable means established by the controller and described to the consumer in
10 the controller's privacy notice pursuant to subsection 2415e(c) of this
11 subchapter.

12 (2)(A) A consumer may designate another person to serve as the
13 consumer's authorized agent, and act on the consumer's behalf, to opt out of
14 the processing of the consumer's personal data for the purposes specified in
15 subsection (a) of this section.

16 (B) The consumer may designate an authorized agent by way of,
17 among other things, a technology, including an internet link or a browser
18 setting, browser extension, or global device setting, indicating the consumer's
19 intent to opt out of the processing.

20 (C) A controller shall comply with an opt-out request received from
21 an authorized agent if the controller is able to verify, with commercially

1 reasonable effort, the identity of the consumer and the authorized agent's
2 authority to act on the consumer's behalf.

3 (3) In the case of processing personal data of a consumer who:

4 (A) a controller has actual knowledge, or willfully disregards, is a
5 child, the parent or legal guardian may exercise the consumer rights on the
6 child's behalf; and

7 (B) is subject to a guardianship, conservatorship, or other protective
8 arrangement, the guardian or the conservator of the consumer may exercise the
9 rights on the consumer's behalf.

10 (c) Controller compliance. Except as otherwise provided in this
11 subchapter, a controller shall comply with a request by a consumer to exercise
12 the consumer rights authorized pursuant to this subchapter as follows:

13 (1) Timeline to respond. A controller:

14 (A) shall respond to the consumer without undue delay, but not later
15 than 45 days after receipt of the request; and

16 (B) may extend the response period by 45 additional days when
17 reasonably necessary, considering the complexity and number of the
18 consumer's requests, provided the controller informs the consumer of the
19 extension within the initial 45-day response period and of the reason for the
20 extension.

1 (2) Declining to take action. If a controller declines to take action
2 regarding the consumer's request, the controller shall inform the consumer
3 without undue delay, but not later than 45 days after receipt of the request, of
4 the justification for declining to take action and instructions for how to appeal
5 the decision.

6 (3) Cost of information.

7 (A) Information provided by a controller in response to a consumer
8 request shall be provided by the controller, free of charge, once per consumer
9 during any 12-month period.

10 (B) If requests from a consumer are manifestly unfounded, excessive,
11 or repetitive, the controller may charge the consumer a reasonable fee to cover
12 the administrative costs of complying with the request or decline to act on the
13 request.

14 (C) The controller bears the burden of demonstrating the manifestly
15 unfounded, excessive, or repetitive nature of the request.

16 (4) Authentication of request.

17 (A) If a controller is unable to authenticate a request to exercise any
18 of the rights afforded under subdivisions (a)(1)–(4) of this section using
19 commercially reasonable efforts, the controller shall not be required to comply
20 with a request to initiate an action pursuant to this section and shall provide
21 notice to the consumer that the controller is unable to authenticate the request

1 to exercise the right or rights until the consumer provides additional
2 information reasonably necessary to authenticate the consumer and the
3 consumer's request to exercise the right or rights.

4 (B) A controller shall not be required to authenticate an opt-out
5 request, but a controller may deny an opt-out request if the controller has a
6 good faith, reasonable, and documented belief that the request is fraudulent.

7 (C) If a controller denies an opt-out request because the controller
8 believes the request is fraudulent, the controller shall send a notice to the
9 person who made the request disclosing that the controller believes the request
10 is fraudulent, why the controller believes the request is fraudulent, and that the
11 controller shall not comply with the request.

12 (5) Third-party data. A controller that has obtained personal data about
13 a consumer from a source other than the consumer shall be deemed in
14 compliance with a consumer's request to delete the consumer's data pursuant
15 to subdivision (a)(3) of this section by:

16 (A) retaining a record of the deletion request and the minimum data
17 necessary for the purpose of ensuring the consumer's personal data remains
18 deleted from the controller's records and not using the retained data for any
19 other purpose pursuant to the provisions of this subchapter; or

1 (B) opting the consumer out of the processing of the personal data for
2 any purpose except for those exempted pursuant to the provisions of this
3 subchapter.

4 (d) Appeals.

5 (1) A controller shall establish a process for a consumer to appeal the
6 controller's refusal to take action on a request pursuant to this section within a
7 reasonable period of time after the consumer's receipt of the decision.

8 (2) The appeal process shall be conspicuously available and similar to
9 the process for submitting requests to initiate action pursuant to this section.

10 (3) Not later than 60 days after receipt of an appeal, a controller shall
11 inform the consumer in writing of any action taken or not taken in response to
12 the appeal, including a written explanation of the reasons for the decisions.

13 (4) If the controller denies the appeal, the controller shall also provide
14 the consumer with an online mechanism, if available, or other method through
15 which the consumer may contact the Attorney General to submit a complaint.

16 (e) Disclosure of certain information. A controller shall not disclose the
17 following personal data in response to a request to exercise the consumer's
18 rights pursuant to subdivision (a)(1) of this section and shall instead inform the
19 consumer or the person exercising such right on behalf of the consumer, with
20 sufficient particularity, that the controller has collected the consumer's:

1 (1) Social Security number;

2 (2) driver's license number, State identification card number, or other
3 government-issued identification number;

4 (3) financial account number;

5 (4) health insurance identification number or medical identification
6 number;

7 (5) account password;

8 (6) security question or answer thereto; or

9 (7) biometric data.

10 § 2415e. DUTIES OF CONTROLLERS

11 (a) Data collection and processing. A controller shall:

12 (1) limit the collection of a consumer's personal data to what is
13 reasonably necessary and proportionate in relation to the purposes for which
14 the data are processed, as disclosed to the consumer;

15 (2) not process a consumer's personal data for any material new purpose
16 that is neither reasonably necessary to, nor compatible with, the purposes for
17 which the data were processed pursuant to subdivision (1) of this subsection,
18 unless the controller receives consent from the consumer;

19 (3) establish, implement, and maintain reasonable administrative,
20 technical, and physical data security practices to protect the confidentiality,

1 integrity, and accessibility of personal data appropriate to the volume and
2 nature of the personal data at issue;

3 (4) regarding the sensitive data of a consumer:

4 (A) not process the sensitive data unless the consumer has provided
5 consent and unless the processing is reasonably necessary in relation to the
6 purposes for which the sensitive data are collected;

7 (B) not sell the sensitive data unless the consumer has provided
8 consent; and

9 (C) if the controller has actual knowledge, or willfully disregards,
10 that the consumer is a child, process the sensitive data in accordance with:

11 (i) COPPA; and

12 (ii) if applicable, section 2449f of this title;

13 (5) not process personal data in violation of any:

14 (A) law of this State that prohibits unlawful discrimination against
15 consumers and any evidence, or lack of evidence, concerning proactive
16 antibias testing or any similar proactive effort to avoid processing data in
17 violation of any such law, including any evidence or lack of evidence
18 concerning the quality, efficacy, recency, and scope of any testing or effort, the
19 results of which shall be relevant to any claim available for a violation of such
20 law and any defense available thereto; or

1 (B) federal law that prohibits unlawful discrimination against
2 consumers;

3 (6) provide an effective mechanism for a consumer to revoke the
4 consumer's consent under this section that is at least as easy as the mechanism
5 by which the consumer provided the consumer's consent and, upon revocation
6 of the consent, cease to process the data as soon as practicable, but not later
7 than 15 days after the receipt of the request;

8 (7) subject to subdivision (9) of this subsection, if a controller has actual
9 knowledge, and willfully disregards, that a consumer is at least 13 years of age
10 but younger than 18 years of age:

11 (A) not process the personal data of the consumer for purposes of
12 targeted advertising; and

13 (B) not sell the consumer's personal data;

14 (8) not discriminate against a consumer for exercising any of the
15 consumer rights contained in this subchapter, including denying goods or
16 services, charging different prices or rates for goods or services, or providing a
17 different level of quality of goods or services to the consumer; and

18 (9) if the controller is a covered business and the consumer is a covered
19 minor as both terms are defined in section 2449a of this title, comply with the
20 requirements set forth in chapter 62, subchapter 6 of this title (Vermont Age-
21 Appropriate Design Code Act).

1 (b) Limitations. Subsection (a) of this section shall not be construed to:

2 (1) require a controller to provide a product or service that requires the
3 personal data of a consumer that the controller does not collect or maintain; or

4 (2) prohibit a controller from offering a different price, rate, level,
5 quality, or selection of goods or services to a consumer, including offering
6 goods or services for no fee if the offering is in connection with a consumer's
7 voluntary participation in a bona fide loyalty, rewards, premium features,
8 discounts, or club card program.

9 (c) Privacy notice.

10 (1) A controller shall provide consumers with a reasonably accessible,
11 clear, and meaningful privacy notice that includes:

12 (A) the categories of personal data processed by the controller;

13 (B) the purpose for processing personal data and a description of the
14 processing, pursuant to subdivision (a)(1) of this section;

15 (C) a description of the means, established pursuant to subsection (d)
16 of this section, for consumers to submit requests to exercise their consumer
17 rights pursuant to this subchapter, including a description of how consumers
18 may:

19 (i) exercise a consumer's rights under subsection 2415d(a) of this
20 subchapter; and

1 (ii) appeal a controller’s decisions with regard to requests to
2 exercise such rights;

3 (D) the categories of personal data that the controller sells to third
4 parties, if any;

5 (E) the categories of third parties, if any, to which the controller sells
6 personal data;

7 (F) a clear and conspicuous disclosure of any:

8 (i) processing of personal data for purposes of targeted
9 advertising; or

10 (ii) sale of personal data to a third party for purposes of targeted
11 advertising;

12 (G) an active email address or other online mechanism that the
13 consumer may use to contact the controller;

14 (H) a statement disclosing whether the controller collects, uses, or
15 sells personal data for the purpose of training large language models; and

16 (I) the most recent month and year during which the controller
17 updated the privacy notice.

18 (2) A controller shall make the privacy notice required under
19 subdivision (1) of this subsection publicly available:

20 (A) through a conspicuous hyperlink that includes the word
21 “privacy”:

1 (i) on the home page of the controller’s website, if the controller
2 maintains a website;

3 (ii) on the application store page or download page of a mobile
4 device, if the controller maintains an application for use on a mobile device;
5 and

6 (iii) on the application’s settings menu or in a similarly
7 conspicuous and accessible location, if the controller maintains an application
8 for use on a mobile device or other device used to connect to the internet;

9 (B) through a medium in which the controller regularly interacts with
10 consumers, including mail, if the controller does not maintain a website;

11 (C) in each language in which the controller:

12 (i) provides any product or service that is subject to the privacy
13 notice; or

14 (ii) carries out any activity that is related to any product or service
15 described in subdivision (i) of this subdivision (C); and

16 (D) in a manner that is reasonably accessible to, and usable by,
17 individuals with disabilities.

18 (3) Whenever a controller makes any retroactive material change to the
19 controller’s privacy notice or practices, the controller shall:

1 (A) notify the consumers affected by such material change with
2 respect to any personal data to be collected after the effective date of such
3 material change;

4 (B) provide a reasonable opportunity for the consumers described in
5 subdivision (A) of this subdivision (3) to withdraw consent to any further and
6 materially different collection, processing, or transfer of previously collected
7 personal data following such material change; and

8 (C) take all reasonable electronic measures to provide the notice set
9 forth in this subdivision (3) to the affected consumers, taking into account the
10 technology available to the controller and the nature of the controller's
11 relationship with such affected consumers.

12 (4) Nothing in this subsection shall be construed to require a controller
13 to provide a privacy notice that is specific to this State if the controller
14 provides a generally applicable privacy notice that satisfies the requirements
15 established in this subsection.

16 (d) Providing consumers access to exercise rights.

17 (1) A controller shall:

18 (A) establish and describe in a privacy notice, one or more secure and
19 reliable means for consumers to submit a request to exercise their consumer
20 rights pursuant to this subchapter; and

1 (B) not require a consumer to create a new account in order to
2 exercise consumer rights but may require a consumer to use an existing
3 account.

4 (2) The means pursuant to subdivision (1) of this subsection shall:

5 (A) take into account the ways in which consumers normally interact
6 with the controller, the need for secure and reliable communication of the
7 requests, and the ability of the controller to verify the identity of the consumer
8 making the request;

9 (B) provide a clear and conspicuous link on the controller's website
10 to a web page that enables a consumer, or an agent of the consumer, to opt out
11 of the processing of the consumer's personal data for purposes of targeted
12 advertising or any sale of the consumer's personal data; and

13 (C) allow a consumer to opt out of any processing of the consumer's
14 personal data for the purposes of targeted advertising, or any sale of the
15 personal data, through an opt-out preference signal sent to the controller with
16 the consumer's consent indicating the consumer's intent to opt out of any of
17 the processing or sale, by a platform, technology, or other mechanism that
18 shall:

19 (i) not unfairly disadvantage another controller;

20 (ii) not make use of a default setting, but rather require the

21 consumer to make an affirmative, freely given, and unambiguous choice to opt

1 out of any processing of the consumer's personal data pursuant to this
2 subchapter;

3 (iii) be consumer friendly and easy to use by the average
4 consumer;

5 (iv) be as consistent as possible with any other similar platform,
6 technology, or mechanism required by any federal or State law or regulation;
7 and

8 (v) enable the controller to accurately determine whether the
9 consumer is a resident of this State and whether the consumer has made a
10 legitimate request to opt out of any sale of the consumer's personal data or
11 targeted advertising.

12 (3) If a consumer's decision to opt out of any processing of the
13 consumer's personal data for the purposes of targeted advertising, or any sale
14 of the personal data, through an opt-out preference signal sent in accordance
15 with the provisions of subdivision (2)(C) of this subsection conflicts with the
16 consumer's existing controller-specific privacy setting or voluntary
17 participation in a controller's bona fide loyalty, rewards, premium features,
18 discounts, or club card program, the controller shall comply with the
19 consumer's opt-out preference signal but may notify the consumer of the
20 conflict and provide to the consumer the choice to confirm the controller-
21 specific privacy setting or participation in the program.

1 (4) If a controller responds to a consumer opt-out request received
2 pursuant to subdivision (2)(C) of this subsection by informing the consumer of
3 a charge for the use of any product or service, the controller shall present the
4 terms of any financial incentive offered pursuant to subdivision (b)(2) of this
5 section for the retention, use, sale, or sharing of the consumer’s personal data.

6 § 2415f. PROCESSORS’ DUTIES; CONTRACTS BETWEEN

7 CONTROLLERS AND PROCESSORS

8 (a) Generally. A processor shall adhere to the instructions of a controller
9 and shall assist the controller in meeting the controller’s obligations under this
10 subchapter, including:

11 (1) taking into account the nature of processing and to the extent
12 possible, to fulfill the controller’s obligation to respond to consumer rights
13 requests pursuant to subsection 2415d(a) of this subchapter;

14 (2) taking into account the nature of processing and the information
15 available to the processor, by assisting the controller in meeting the
16 controller’s obligations in relation to the security of processing the personal
17 data and in relation to the notification of a data broker security breach or
18 security breach, as defined in section 2430 of this title, of the system of the
19 processor, in order to meet the controller’s obligations; and

20 (3) providing necessary information to enable the controller to conduct
21 and document data protection and impact assessments.

1 (b) Contractual terms.

2 (1) A contract between a controller and a processor shall govern the
3 processor's data processing procedures with respect to processing performed
4 on behalf of the controller.

5 (2) The contract shall be binding and clearly set forth instructions for
6 processing data, the nature and purpose of processing, the type of data subject
7 to processing, the duration of processing, and the rights and obligations of both
8 parties.

9 (3) The contract shall require that the processor:

10 (A) ensure that each person processing personal data is subject to a
11 duty of confidentiality with respect to the data;

12 (B) at the controller's direction, delete or return all personal data to
13 the controller as requested at the end of the provision of services, unless
14 retention of the personal data is required by law;

15 (C) upon the reasonable request of the controller, make available to
16 the controller all information in its possession necessary to demonstrate the
17 processor's compliance with the obligations in this subchapter;

18 (D) after providing the controller an opportunity to object, engage
19 any subcontractor pursuant to a written contract that requires the subcontractor
20 to meet the obligations of the processor with respect to the personal data; and

1 (E) make available to the controller upon the reasonable request of
2 the controller all information in the processor's possession necessary to
3 demonstrate the processor's compliance with this subchapter.

4 (4) A processor shall provide a report of an assessment to the controller
5 upon request.

6 (c) Liabilities. This section shall not be construed to relieve a controller or
7 processor from the liabilities imposed on the controller or processor by virtue
8 of the controller's or processor's role in the processing relationship, as
9 described in this subchapter.

10 (d) Processors performing as controllers.

11 (1) Determining whether a person is acting as a controller or processor
12 with respect to a specific processing of data is a fact-based determination that
13 depends upon the context in which personal data are to be processed.

14 (2) A person who is not limited in the person's processing of personal
15 data pursuant to a controller's instructions, or who fails to adhere to the
16 instructions, is a controller and not a processor with respect to a specific
17 processing of data.

18 (3) A processor that continues to adhere to a controller's instructions
19 with respect to a specific processing of personal data remains a processor.

20 (4) If a processor begins, alone or jointly with others, determining the
21 purposes and means of the processing of personal data, the processor is a

1 controller with respect to the processing and may be subject to an enforcement
2 action under section 2415j of this subchapter.

3 § 2415g. DATA PROTECTION AND IMPACT ASSESSMENTS;

4 DISCLOSURE TO ATTORNEY GENERAL

5 (a) Generally. A controller shall conduct and document a data protection
6 assessment for each of the controller's processing activities that presents a
7 heightened risk of harm to a consumer, which for the purposes of this section
8 includes:

9 (1) the processing of personal data for the purposes of targeted
10 advertising;

11 (2) the sale of personal data;

12 (3) the processing of personal data for the purposes of profiling, if the
13 profiling presents a reasonably foreseeable risk of:

14 (A) unfair or deceptive treatment of, or unlawful disparate impact on,
15 a consumer;

16 (B) financial, physical, or reputational injury to a consumer;

17 (C) a physical or other intrusion upon the solitude or seclusion, or the
18 private affairs or concerns, of a consumer, if the intrusion would be offensive
19 to a reasonable person; or

20 (D) other substantial injury to a consumer; and

21 (4) the processing of sensitive data.

1 (b) Requirements.

2 (1) Data protection assessments conducted pursuant to subsection (a) of
3 this section shall identify and weigh the benefits that may flow, directly and
4 indirectly, from the processing to the controller, the consumer, other
5 stakeholders, and the public against the potential risks to the rights of the
6 consumer associated with the processing, as mitigated by safeguards that can
7 be employed by the controller to reduce the risks.

8 (2) The controller shall factor into each data protection assessment the
9 use of deidentified data and the reasonable expectations of consumers, as well
10 as the context of the processing and the relationship between the controller and
11 the consumer whose personal data will be processed.

12 (c) Impact assessments for profiling. Each controller that engages in any
13 profiling for the purposes of making a decision that produces any legal or
14 similarly significant effect concerning a consumer shall conduct an impact
15 assessment for the profiling. The impact assessment shall include, to the
16 extent reasonably known by or available to the controller, as applicable:

17 (1) a statement by the controller disclosing the purpose, intended use
18 cases, and deployment context of, and benefits afforded by, the profiling;

19 (2) an analysis of whether the profiling poses any known or reasonably
20 foreseeable heightened risk of harm to a consumer, and, if so:

- 1 (A) the nature of such heightened risk of harm to a consumer; and
- 2 (B) the steps that have been taken to mitigate such heightened risk of
3 harm to a consumer;
- 4 (3) a description of:
- 5 (A) the main categories of personal data processed as inputs for the
6 purposes of such profiling; and
- 7 (B) the outputs such profiling produces;
- 8 (4) an overview of the main categories of personal data the controller
9 used to customize the profiling, if the controller used data to customize the
10 profiling;
- 11 (5) any metrics used to evaluate the performance and known limitations
12 of the profiling;
- 13 (6) a description of any transparency measures taken concerning the
14 profiling, including any measures taken to disclose to consumers that the
15 controller is engaged in profiling while the controller is engaged in the
16 profiling; and
- 17 (7) a description of the postdeployment monitoring and user safeguards
18 provided concerning such profiling, including the oversight, use, and learning
19 processes established by the controller to address issues arising from such
20 profiling.

1 (d) Disclosure to Attorney General.

2 (1) The Attorney General may require that a controller disclose any data
3 protection or impact assessment that is relevant to an investigation conducted
4 by the Attorney General, and the controller shall make the data protection or
5 impact assessment available to the Attorney General.

6 (2) The Attorney General may evaluate the data protection or impact
7 assessment for compliance with the responsibilities set forth in this subchapter.

8 (3) Data protection and impact assessments shall be confidential and
9 shall be exempt from disclosure and copying under the Public Records Act.

10 (4) To the extent any information contained in a data protection or
11 impact assessment disclosed to the Attorney General includes information
12 subject to attorney-client privilege or work product protection, the disclosure
13 shall not constitute a waiver of the privilege or protection.

14 (e) Assessment efficiency and applicability.

15 (1) A single data protection or impact assessment may address a
16 comparable set of processing operations that include similar activities.

17 (2) If a controller conducts a data protection or impact assessment for
18 the purpose of complying with another applicable law or regulation, the data
19 protection or impact assessment shall be deemed to satisfy the requirements
20 established in this section if the data protection or impact assessment is

1 reasonably similar in scope and effect to the data or impact protection
2 assessment that would otherwise be conducted pursuant to this section.

3 (3) Data protection and impact assessment requirements shall apply to
4 processing activities created or generated after January 1, 2028, and are not
5 retroactive.

6 § 2415h. DEIDENTIFIED DATA

7 (a) Requirements. A controller in possession of deidentified data shall:

8 (1) take reasonable measures to ensure that the data cannot be associated
9 with an individual;

10 (2) publicly commit to maintaining and using deidentified data without
11 attempting to reidentify the data; and

12 (3) contractually obligate any recipients of the deidentified data to
13 comply with the provisions of this subchapter.

14 (b) Limitations. This subchapter shall not be construed to:

15 (1) require a controller or processor to reidentify deidentified data or
16 pseudonymous data;

17 (2) maintain data in identifiable form, or collect, obtain, retain, or access
18 any data or technology, in order to be capable of associating an authenticated
19 consumer request with personal data; or

20 (3) require a controller or processor to comply with an authenticated
21 consumer rights request if the controller:

1 (A) is not reasonably capable of associating the request with the
2 personal data or it would be unreasonably burdensome for the controller to
3 associate the request with the personal data;

4 (B) does not use the personal data to recognize or respond to the
5 specific consumer who is the subject of the personal data, or associate the
6 personal data with other personal data about the same specific consumer; and

7 (C) does not sell the personal data to any third party or otherwise
8 voluntarily disclose the personal data to any third party other than a processor,
9 except as otherwise permitted in this section.

10 (c) Pseudonymous data. The rights afforded under subdivisions
11 2415d(a)(1)–(4) of this subchapter shall not apply to pseudonymous data in
12 cases in which the controller is able to demonstrate that any information
13 necessary to identify the consumer is kept separately and is subject to effective
14 technical and organizational controls that prevent the controller from accessing
15 the information.

16 (d) Oversight when disclosing. A controller that discloses pseudonymous
17 data or deidentified data shall exercise reasonable oversight to monitor
18 compliance with any contractual commitments to which the pseudonymous
19 data or deidentified data is subject and shall take appropriate steps to address
20 any breaches of those contractual commitments.

1 § 2415i. CONSTRUCTION OF DUTIES

2 (a) Generally. This subchapter shall not be construed to restrict a
3 controller's, processor's, or consumer health data controller's ability to:

4 (1) comply with federal, state, or municipal laws, ordinances, or
5 regulations, except as prohibited by 1 V.S.A. § 150;

6 (2) comply with a civil, criminal, or regulatory inquiry, investigation,
7 subpoena, or summons by federal, state, municipal, or other governmental
8 authorities;

9 (3) cooperate with law enforcement agencies concerning conduct or
10 activity that the controller, processor, or consumer health data controller
11 reasonably and in good faith believes may violate federal, state, or municipal
12 laws, ordinances, or regulations;

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

14 (5) provide a product or service specifically requested by a consumer;

15 (6) perform under a contract to which a consumer is a party, including
16 fulfilling the terms of a written warranty;

17 (7) take steps at the request of a consumer prior to entering into a
18 contract;

19 (8) take immediate steps to protect an interest that is essential for the life
20 or physical safety of the consumer or another individual, and if the processing
21 cannot be manifestly based on another legal basis;

1 (9) prevent, detect, protect against, or respond to security incidents,
2 identity theft, fraud, harassment, malicious or deceptive activities, or any
3 illegal activity; preserve the integrity or security of systems; or investigate,
4 report, or prosecute those responsible for the action;

5 (10) engage in public or peer-reviewed scientific or statistical research
6 in the public interest that adheres to all other applicable ethics and privacy laws
7 and is approved, monitored, and governed by an institutional review board that
8 determines, or similar independent oversight entities that determine:

9 (A) whether the deletion of the information is likely to provide
10 substantial benefits that do not exclusively accrue to the controller;

11 (B) the expected benefits of the research outweigh the privacy risks;
12 and

13 (C) whether the controller or consumer health data controller has
14 implemented reasonable safeguards to mitigate privacy risks associated with
15 research, including any risks associated with reidentification;

16 (11) assist another controller, processor, consumer health data
17 controller, or third party with any of the obligations under this subchapter; or

18 (12) process personal data for reasons of public interest in the area of
19 public health, community health, or population health, but solely to the extent
20 that the processing is:

1 (A) subject to suitable and specific measures to safeguard the rights
2 of the consumer whose personal data are being processed; and

3 (B) under the responsibility of a professional subject to
4 confidentiality obligations under federal, state, or local law.

5 (b) Internal use of data. The obligations imposed on controllers,
6 processors, or consumer health data controllers under this subchapter shall not
7 restrict a controller's, processor's, or consumer health data controller's ability
8 to collect, use, or retain data for internal use to:

9 (1) conduct internal research to develop, improve, or repair products,
10 services, or technology;

11 (2) effectuate a product recall;

12 (3) identify and repair technical errors that impair existing or intended
13 functionality;

14 (4) process personal data for the purposes of profiling in furtherance of
15 any automated decision that may produce any legal or similarly significant
16 effect concerning a consumer, provided the personal data are:

17 (A) processed only to the extent necessary to detect or correct any
18 bias that may result from processing the data for such purposes, the bias cannot
19 effectively be detected or corrected without processing the data, and the data
20 are deleted once the processing has been completed;

1 (B) processed subject to appropriate safeguards to protect the rights
2 of consumers secured by the Constitution or laws of this State or of the United
3 States;

4 (C) subject to technical restrictions concerning the reuse of the data
5 and industry-standard security and privacy measures, including
6 pseudonymization;

7 (D) subject to measures to ensure that the data are secure, protected,
8 and subject to suitable safeguards, including strict controls concerning, and
9 documentation of, access to the data, to avoid misuse and ensure that only
10 authorized persons may access the data while preserving the confidentiality of
11 the data; and

12 (E) not transmitted, transferred, or otherwise accessed by any third
13 party;

14 (5) perform internal operations that are reasonably aligned with the
15 expectations of the consumer or reasonably anticipated based on the
16 consumer's existing relationship with the controller or consumer health data
17 controller, or are otherwise compatible with processing data in furtherance of
18 the provision of a product or service specifically requested by a consumer or
19 the performance of a contract to which the consumer is a party; or

20 (6) perform internal operations in accordance with the internal
21 operations exception established in COPPA if the controller, processor, or

1 consumer health data controller is processing data in accordance with the
2 exception.

3 (c) Evidentiary privilege.

4 (1) The obligations imposed on controllers, processors, or consumer
5 health data controllers under this subchapter shall not apply if compliance by
6 the controller, processor, or consumer health data controller with this
7 subchapter would violate an evidentiary privilege under the laws of this State.

8 (2) This subchapter shall not be construed to prevent a controller,
9 processor, or consumer health data controller from providing personal data
10 concerning a consumer to a person covered by an evidentiary privilege under
11 the laws of this State as part of a privileged communication.

12 (3) Nothing in this subchapter modifies 2020 Acts and Resolves No.
13 166, Sec. 14 or authorizes the use of facial recognition technology by law
14 enforcement.

15 (d) Third parties.

16 (1) A controller, processor, or consumer health data controller that
17 discloses personal data to a processor or third-party controller pursuant to this
18 subchapter shall not be deemed to have violated this subchapter if the
19 processor or third-party controller that receives and processes the personal data
20 violates this subchapter, provided, at the time the disclosing controller,
21 processor, or consumer health data controller disclosed the personal data, the

1 disclosing controller, processor, or consumer health data controller did not
2 have actual knowledge that the receiving processor or third-party controller
3 would violate this subchapter.

4 (2) A third-party controller or processor receiving personal data from a
5 controller, processor, or consumer health data controller in compliance with
6 this subchapter is not in violation of this subchapter for the transgressions of
7 the controller, processor, or consumer health data controller from which the
8 third-party controller or processor receives the personal data.

9 (e) Clarifications. This subchapter shall not be construed to:

10 (1) impose any obligation on a controller or processor that adversely
11 affects the rights or freedoms of any person, including the rights of any person:

12 (A) to freedom of speech or freedom of the press guaranteed in the
13 First Amendment to the U.S. Constitution; or

14 (B) under 12 V.S.A. § 1615;

15 (2) apply to any person's processing of personal data in the course of the
16 person's purely personal or household activities; or

17 (3) require an independent school as defined in 16 V.S.A. § 11(a)(8) or a
18 private institution of higher education, as defined in 20 U.S.C. § 1001 et seq.,
19 to delete personal data or opt out of processing of personal data that would
20 unreasonably interfere with the provision of education services by or the
21 ordinary operation of the school or institution.

1 (f) Personal data processing.

2 (1) Personal data processed by a controller or consumer health data
3 controller pursuant to this section may be processed to the extent that the
4 processing is:

5 (A) reasonably necessary and proportionate to the purposes listed in
6 this section; and

7 (B) adequate, relevant, and limited to what is necessary in relation to
8 the specific purposes listed in this section.

9 (2)(A) The collection, use, or retention of personal data pursuant to
10 subsection (b) of this section shall, where applicable, take into account the
11 nature and purpose or purposes of the collection, use, or retention.

12 (B) The data shall be subject to reasonable administrative, technical,
13 and physical measures to protect the confidentiality, integrity, and accessibility
14 of the personal data and to reduce reasonably foreseeable risks of harm to
15 consumers relating to the collection, use, or retention of personal data.

16 (3) If a controller or consumer health data controller processes personal
17 data pursuant to an exemption in this section, the controller or consumer health
18 data controller bears the burden of demonstrating that the processing qualifies
19 for the exemption and complies with the requirements of this subsection.

1 (4) Processing personal data for the purposes expressly identified in this
2 section shall not solely make a legal entity a controller or consumer health data
3 controller with respect to the processing.

4 § 2415j. ATTORNEY GENERAL ENFORCEMENT; REPORTING

5 (a) Consumer Protection Act. A violation of this subchapter shall be
6 deemed a violation of the Vermont Consumer Protection Act, pursuant to
7 chapter 63 of this title. The Attorney General has the same authority to enforce
8 this subchapter as provided under 9 V.S.A. chapter 63, subchapter 1. This
9 subchapter shall not be construed as providing the basis for, or be subject to, a
10 private right of action for violations of this subchapter or any other law.

11 (b) Reporting. Annually, on or before December 1, the Attorney General
12 shall submit a report to the General Assembly disclosing:

13 (1) the number of notices of violation pursuant to this subchapter that
14 the Attorney General has issued;

15 (2) the nature of each violation;

16 (3) the number of violations that resulted in an enforcement action being
17 taken;

18 (4) the number of enforcement actions that proceeded to trial;

19 (5) whether and to what extent the Attorney General has offered an
20 opportunity for a controller or processor to cure a violation; and

1 (6) any other matter the Attorney General deems relevant for the
2 purposes of the report.

3 (c) Guidance. The Attorney General shall provide, and update as
4 necessary, guidance to controllers and processors for compliance with the
5 terms of the Vermont Data Privacy and Online Surveillance Act.

6 § 2415k. CONSUMER HEALTH DATA PRIVACY

7 A person shall not:

8 (1) provide any employee or contractor with access to consumer health
9 data unless the employee or contractor is subject to a contractual or statutory
10 duty of confidentiality;

11 (2) provide any processor with access to consumer health data unless the
12 person and processor comply with section 2415f of this subchapter;

13 (3) use a geofence to establish a virtual boundary that is within 1,850
14 feet of any health care facility, including any mental health facility or
15 reproductive or sexual health facility, for the purpose of identifying, tracking,
16 collecting data from, or sending any notification to a consumer regarding the
17 consumer's consumer health data; or

18 (4) sell, or offer to sell, consumer health data without first obtaining the
19 consumer's consent.

1 Sec. 2. DATA PRIVACY; INTENT; ENFORCEMENT; EDUCATION

2 (a) Enforcement intent. Through this act, the General Assembly makes the
3 decision to not provide consumers with a right to hold persons accountable in
4 civil court for violations of the Vermont Data Privacy and Online Surveillance
5 Act. Consequently, the Office of the Attorney General will bear the burden of
6 enforcing the Act and ensuring, to the best of its abilities, that the rights of
7 Vermonters will be protected. In prohibiting a private right of action, it is the
8 intent of the General Assembly that additional appropriations and resources
9 will be provided in the following years to support the Office of the Attorney
10 General's enforcement of this Act, which may require the creation of a data
11 privacy unit. If such appropriations or resources are not provided, the General
12 Assembly may consider adding a private right of action for consumers.

13 (b) Educational intent. It is also the intent of the General Assembly that
14 appropriate educational resources and sufficient technical support will be
15 provided by the State in the following years to help Vermont businesses
16 comply with the Act.

17 Sec. 3. DATA PRIVACY; ENFORCEMENT; CURE PERIOD

18 During the period beginning January 1, 2028, and ending on June 30, 2029,
19 the Attorney General shall, prior to initiating any action for a violation of the
20 Vermont Data Privacy and Online Surveillance Act, issue a notice of violation
21 to the alleged violator if the Attorney General determines that a cure is

1 possible. If the person fails to cure the violation within 60 days after receipt of
2 the notice of violation, the Attorney General may bring an action pursuant to
3 9 V.S.A. § 2415j(a).

4 Sec. 4. EFFECTIVE DATE

5 This act shall take effect on January 1, 2028.