H.121 Page 1 of 39

1	H.121
2	An act relating to enhancing consumer privacy
3	The Senate concurs in the House proposal of amendment to Senate proposal
4	of amendment with the following further proposals of amendment thereto:
5	First: In Sec. 1, 9 V.S.A. chapter 61A, by striking out section 2415 in its
6	entirety and inserting in lieu thereof a new section 2415 to read as follows:
7	§ 2415. DEFINITIONS
8	As used in this chapter:
9	(1)(A) "Affiliate" means a legal entity that shares common branding
10	with another legal entity or controls, is controlled by, or is under common
11	control with another legal entity.
12	(B) As used in subdivision (A) of this subdivision (1), "control" or
13	"controlled" means:
14	(i) ownership of, or the power to vote, more than 50 percent of the
15	outstanding shares of any class of voting security of a company;
16	(ii) control in any manner over the election of a majority of the
17	directors or of individuals exercising similar functions; or
18	(iii) the power to exercise controlling influence over the
19	management of a company.

1	(2) "Age estimation" means a process that estimates that a consumer is
2	likely to be of a certain age, fall within an age range, or is over or under a
3	certain age.
4	(A) Age estimation methods include:
5	(i) analysis of behavioral and environmental data the controller
6	already collects about its consumers;
7	(ii) comparing the way a consumer interacts with a device or with
8	consumers of the same age;
9	(iii) metrics derived from motion analysis; and
10	(iv) testing a consumer's capacity or knowledge.
11	(B) Age estimation does not require certainty, and if a controller
12	estimates a consumer's age for the purpose of advertising or marketing, that
13	estimation may also be used to comply with this chapter.
14	(3) "Age verification" means a system that relies on hard identifiers or
15	verified sources of identification to confirm a consumer has reached a certain
16	age, including government-issued identification or a credit card.
17	(4) "Authenticate" means to use reasonable means to determine that a
18	request to exercise any of the rights afforded under subdivisions 2418(a)(1)-
19	(5) of this title is being made by, or on behalf of, the consumer who is entitled
20	to exercise the consumer rights with respect to the personal data at issue.

H.121 Page 3 of 39

1	(5)(A) "Biometric data" means data generated from the technological
2	processing of an individual's unique biological, physical, or physiological
3	characteristics that is linked or reasonably linkable to an individual, including:
4	(i) iris or retina scans;
5	(ii) fingerprints;
6	(iii) facial or hand mapping, geometry, or templates;
7	(iv) vein patterns;
8	(v) voice prints; and
9	(vi) gait or personally identifying physical movement or patterns.
10	(B) "Biometric data" does not include:
11	(i) a digital or physical photograph;
12	(ii) an audio or video recording; or
13	(iii) any data generated from a digital or physical photograph, or
14	an audio or video recording, unless such data is generated to identify a specific
15	individual.
16	(6) "Broker-dealer" has the same meaning as in 9 V.S.A. § 5102.
17	(7) "Business associate" has the same meaning as in HIPAA.
18	(8) "Child" has the same meaning as in COPPA.

1	(9)(A) "Consent" means a clear affirmative act signifying a consumer's
2	freely given, specific, informed, and unambiguous agreement to allow the
3	processing of personal data relating to the consumer.
4	(B) "Consent" may include a written statement, including by
5	electronic means, or any other unambiguous affirmative action.
6	(C) "Consent" does not include:
7	(i) acceptance of a general or broad terms of use or similar
8	document that contains descriptions of personal data processing along with
9	other, unrelated information;
10	(ii) hovering over, muting, pausing, or closing a given piece of
11	content; or
12	(iii) agreement obtained through the use of dark patterns.
13	(10)(A) "Consumer" means an individual who is a resident of the State.
14	(B) "Consumer" does not include an individual acting in a
15	commercial or employment context or as an employee, owner, director, officer,
16	or contractor of a company, partnership, sole proprietorship, nonprofit, or
17	government agency whose communications or transactions with the controller
18	occur solely within the context of that individual's role with the company,
19	partnership, sole proprietorship, nonprofit, or government agency.

1	(11) "Consumer health data" means any personal data that a controller
2	uses to identify a consumer's physical or mental health condition or diagnosis,
3	including gender-affirming health data and reproductive or sexual health data.
4	(12) "Consumer health data controller" means any controller that, alone
5	or jointly with others, determines the purpose and means of processing
6	consumer health data.
7	(13) "Consumer reporting agency" has the same meaning as in the Fair
8	Credit Reporting Act, 15 U.S.C. § 1681a(f);
9	(14) "Controller" means a person who, alone or jointly with others,
10	determines the purpose and means of processing personal data.
11	(15) "COPPA" means the Children's Online Privacy Protection Act of
12	1998, 15 U.S.C. § 6501-6506, and any regulations, rules, guidance, and
13	exemptions promulgated pursuant to the act, as the act and regulations, rules,
14	guidance, and exemptions may be amended.
15	(16) "Covered entity" has the same meaning as in HIPAA.
16	(17) "Credit union" has the same meaning as in 8 V.S.A. § 30101.
17	(18) "Dark pattern" means a user interface designed or manipulated with
18	the substantial effect of subverting or impairing user autonomy, decision-
19	making, or choice and includes any practice the Federal Trade Commission
20	refers to as a "dark pattern."

1	(19) "Data broker" has the same meaning as in section 2430 of this title.
2	(20) "Decisions that produce legal or similarly significant effects
3	concerning the consumer" means decisions made by the controller that result in
4	the provision or denial by the controller of financial or lending services,
5	housing, insurance, education enrollment or opportunity, criminal justice,
6	employment opportunities, health care services, or access to essential goods or
7	services.
8	(21) "De-identified data" means data that does not identify and cannot
9	reasonably be used to infer information about, or otherwise be linked to, an
10	identified or identifiable individual, or a device linked to the individual, if the
11	controller that possesses the data:
12	(A)(i) takes reasonable measures to ensure that the data cannot be
13	used to re-identify an identified or identifiable individual or be associated with
14	an individual or device that identifies or is linked or reasonably linkable to an
15	individual or household;
16	(ii) for purposes of this subdivision (A), "reasonable measures"
17	shall include the de-identification requirements set forth under 45 C.F.R.
18	§ 164.514 (other requirements relating to uses and disclosures of protected
19	health information);

H.121 Page 7 of 39

1	(B) publicly commits to process the data only in a de-identified
2	fashion and not attempt to re-identify the data; and
3	(C) contractually obligates any recipients of the data to satisfy the
4	criteria set forth in subdivisions (A) and (B) of this subdivision (21).
5	(22) "Financial institution":
6	(A) as used in subdivision 2417(a)(12) of this title, has the same
7	meaning as in 15 U.S.C. § 6809; and
8	(B) as used in subdivision 2417(a)(14) of this title, has the same
9	meaning as in 8 V.S.A. § 11101.
10	(23) "Gender-affirming health care services" has the same meaning as in
11	1 V.S.A. § 150.
12	(24) "Gender-affirming health data" means any personal data
13	concerning a past, present, or future effort made by a consumer to seek, or a
14	consumer's receipt of, gender-affirming health care services, including:
15	(A) precise geolocation data that is used for determining a
16	consumer's attempt to acquire or receive gender-affirming health care services;
17	(B) efforts to research or obtain gender-affirming health care
18	services; and
19	(C) any gender-affirming health data that is derived from nonhealth
20	information.

H.121 Page 8 of 39

1	(25) "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	(26) "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	(27) "Health care component" has the same meaning as in HIPAA.
16	(28) "Health care facility" has the same meaning as in 18 V.S.A. § 9432.
17	(29) "Heightened risk of harm to a minor" means processing the
18	personal data of a minor in a manner that presents a reasonably foreseeable risk
19	of:

H.121 Page 9 of 39

1	(A) unfair or deceptive treatment of, or unlawful disparate impact on,
2	a minor;
3	(B) financial, physical, or reputational injury to a minor;
4	(C) unintended disclosure of the personal data of a minor; or
5	(D) any physical or other intrusion upon the solitude or seclusion, or
6	the private affairs or concerns, of a minor if the intrusion would be offensive to
7	a reasonable person.
8	(30) "HIPAA" means the Health Insurance Portability and
9	Accountability Act of 1996, Pub. L. No. 104-191, and any regulations
10	promulgated pursuant to the act, as may be amended.
11	(31) "Hybrid entity" has the same meaning as in HIPAA.
12	(32) "Identified or identifiable individual" means an individual who can
13	be readily identified, directly or indirectly, including by reference to an
14	identifier such as a name, an identification number, specific geolocation data,
15	or an online identifier.
16	(33) "Independent trust company" has the same meaning as in 8 V.S.A.
17	<u>§ 2401.</u>
18	(34) "Investment adviser" has the same meaning as in 9 V.S.A. § 5102.

H.121 Page 10 of 39

1	(35) "Large data holder" means a person that during the preceding
2	calendar year processed the personal data of not fewer than 100,000
3	consumers.
4	(36) "Mental health facility" means any health care facility in which at
5	least 70 percent of the health care services provided in the facility are mental
6	health services.
7	(37) "Nonpublic personal information" has the same meaning as in
8	15 U.S.C. § 6809.
9	(38)(A) "Online service, product, or feature" means any service,
10	product, or feature that is provided online, except as provided in subdivision
11	(B) of this subdivision (38).
12	(B) "Online service, product, or feature" does not include:
13	(i) telecommunications service, as that term is defined in the
14	Communications Act of 1934, 47 U.S.C. § 153;
15	(ii) broadband internet access service, as that term is defined in
16	47 C.F.R. § 54.400 (universal service support); or
17	(iii) the delivery or use of a physical product.
18	(39) "Patient identifying information" has the same meaning as in
19	42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).

H.121 Page 11 of 39

1	(40) "Patient safety work product" has the same meaning as in 42 C.F.R.
2	§ 3.20 (patient safety organizations and patient safety work product).
3	(41)(A) "Personal data" means any information, including derived data
4	and unique identifiers, that is linked or reasonably linkable to an identified or
5	identifiable individual or to a device that identifies, is linked to, or is
6	reasonably linkable to one or more identified or identifiable individuals in a
7	household.
8	(B) "Personal data" does not include de-identified data or publicly
9	available information.
10	(42)(A) "Precise geolocation data" means information derived from
11	technology that can precisely and accurately identify the specific location of a
12	consumer within a radius of 1,850 feet.
13	(B) "Precise geolocation data" does not include:
14	(i) the content of communications;
15	(ii) data generated by or connected to an advanced utility metering
16	infrastructure system; or
17	(iii) data generated by equipment used by a utility company.
18	(43) "Process" or "processing" means any operation or set of operations
19	performed, whether by manual or automated means, on personal data or on sets

1	of personal data, such as the collection, use, storage, disclosure, analysis,
2	deletion, or modification of personal data.
3	(44) "Processor" means a person who processes personal data on behalf
4	of a controller.
5	(45) "Profiling" means any form of automated processing performed on
6	personal data to evaluate, analyze, or predict personal aspects related to an
7	identified or identifiable individual's economic situation, health, personal
8	preferences, interests, reliability, behavior, location, or movements.
9	(46) "Protected health information" has the same meaning as in HIPAA.
10	(47) "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 is not attributed to
14	an identified or identifiable individual.
15	(48)(A) "Publicly available information" means information that:
16	(i) is lawfully made available through federal, state, or local
17	government records; or
18	(ii) a controller has a reasonable basis to believe that the consumer
19	has lawfully made available to the general public through widely distributed
20	media.

1	(B) "Publicly available information" does not include biometric data
2	collected by a business about a consumer without the consumer's knowledge.
3	(49) "Qualified service organization" has the same meaning as in
4	42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).
5	(50) "Reproductive or sexual health care" has the same meaning as
6	"reproductive health care services" in 1 V.S.A. § 150(c)(1).
7	(51) "Reproductive or sexual health data" means any personal data
8	concerning a past, present, or future effort made by a consumer to seek, or a
9	consumer's receipt of, reproductive or sexual health care.
10	(52) "Reproductive or sexual health facility" means any health care
11	facility in which at least 70 percent of the health care-related services or
12	products rendered or provided in the facility are reproductive or sexual health
13	care.
14	(53)(A) "Sale of personal data" means the exchange of a consumer's
15	personal data by the controller to a third party for monetary or other valuable
16	consideration or otherwise for a commercial purpose.
17	(B) As used in this subdivision (53), "commercial purpose" means to
18	advance a person's commercial or economic interests, such as by inducing
19	another person to buy, rent, lease, join, subscribe to, provide, or exchange

H.121 Page 14 of 39

1	products, goods, property, information, or services, or enabling or effecting,
2	directly or indirectly, a commercial transaction.
3	(C) "Sale of personal data" does not include:
4	(i) the disclosure of personal data to a processor that processes the
5	personal data on behalf of the controller;
6	(ii) the disclosure of personal data to a third party for purposes of
7	providing a product or service requested by the consumer;
8	(iii) the disclosure or transfer of personal data to an affiliate of the
9	controller;
10	(iv) the disclosure of personal data where the consumer directs the
11	controller to disclose the personal data or intentionally uses the controller to
12	interact with a third party;
13	(v) the disclosure of personal data that the consumer:
14	(I) intentionally made available to the general public via a
15	channel of mass media; and
16	(II) did not restrict to a specific audience; or
17	(vi) the disclosure or transfer of personal data to a third party as an
18	asset that is part of a merger, acquisition, bankruptcy or other transaction, or a
19	proposed merger, acquisition, bankruptcy, or other transaction, in which the
20	third party assumes control of all or part of the controller's assets.

H.121 Page 15 of 39

1	(54) "Sensitive data" means personal data that:
2	(A) reveals a consumer's government-issued identifier, such as a
3	Social Security number, passport number, state identification card, or driver's
4	license number, that is not required by law to be publicly displayed;
5	(B) reveals a consumer's racial or ethnic origin, national origin,
6	citizenship or immigration status, religious or philosophical beliefs, or union
7	membership;
8	(C) reveals a consumer's sexual orientation, sex life, sexuality, or
9	status as transgender or nonbinary;
10	(D) reveals a consumer's status as a victim of a crime;
11	(E) is financial information, including a consumer's tax return and
12	account number, financial account log-in, financial account, debit card number
13	or credit card number in combination with any required security or access
14	code, password, or credentials allowing access to an account;
15	(F) is consumer health data;
16	(G) is personal data collected and analyzed concerning consumer
17	health data or personal data that describes or reveals a past, present, or future
18	mental or physical health condition, treatment, disability, or diagnosis,
19	including pregnancy, to the extent the personal data is not used by the

H.121 Page 16 of 39

1	controller to identify a specific consumer's physical or mental health condition
2	or diagnosis;
3	(H) is biometric or genetic data;
4	(I) is personal data collected from a known minor; or
5	(J) is precise geolocation data.
6	(55)(A) "Targeted advertising" means the targeting of an advertisement
7	to a consumer based on the consumer's activity with one or more businesses,
8	distinctly branded websites, applications, or services, other than the controller,
9	distinctly branded website, application, or service with which the consumer is
10	intentionally interacting.
11	(B) "Targeted advertising" does not include:
12	(i) an advertisement based on activities within the controller's own
13	commonly branded website or online application;
14	(ii) an advertisement based on the context of a consumer's current
15	search query, visit to a website, or use of an online application;
16	(iii) an advertisement directed to a consumer in response to the
17	consumer's request for information or feedback; or
18	(iv) processing personal data solely to measure or report
19	advertising frequency, performance, or reach.

H.121 Page 17 of 39

1	(56) "Third party" means a natural or legal person, public authority,
2	agency, or body, other than the consumer, controller, or processor or an
3	affiliate of the processor or the controller.
4	(57) "Trade secret" has the same meaning as in section 4601 of this title.
5	(58) "Victim services organization" means a nonprofit organization that
6	is established to provide services to victims or witnesses of child abuse,
7	domestic violence, human trafficking, sexual assault, violent felony, or
8	stalking.
9	Second: In Sec. 1, 9 V.S.A. chapter 61A, by striking out subsection 2417(a)
10	in its entirety and inserting in lieu thereof a new subsection 2417(a) to read as
11	follows:
12	(a) This chapter does not apply to:
13	(1) a federal, State, tribal, or local government entity in the ordinary
14	course of its operation;
15	(2) a covered entity that is not a hybrid entity, any health care
16	component of a hybrid entity, or a business associate;
17	(3) information used only for public health activities and purposes
18	described in 45 C.F.R. § 164.512 (disclosure of protected health information
19	without authorization);
20	(4) information that identifies a consumer in connection with:

H.121 Page 18 of 39

1	(A) activities that are subject to the Federal Policy for the Protection
2	of Human Subjects, codified as 45 C.F.R. Part 46 (HHS protection of human
3	subjects) and in various other federal regulations;
4	(B) research on human subjects undertaken in accordance with good
5	clinical practice guidelines issued by the International Council for
6	Harmonisation of Technical Requirements for Pharmaceuticals for Human
7	<u>Use;</u>
8	(C) activities that are subject to the protections provided in 21 C.F.R.
9	Parts 50 (FDA clinical investigations protection of human subjects) and
10	56 (FDA clinical investigations institutional review boards); or
11	(D) research conducted in accordance with the requirements set forth
12	in subdivisions (A) through (C) of this subdivision (a)(4) or otherwise in
13	accordance with applicable law;
14	(5) patient identifying information that is collected and processed in
15	accordance with 42 C.F.R. Part 2 (confidentiality of substance use disorder
16	patient records);
17	(6) patient safety work product that is created for purposes of improving
18	patient safety under 42 C.F.R. Part 3 (patient safety organizations and patient
19	safety work product);

H.121 Page 19 of 39

1	(7) information or documents created for the purposes of the Healthcare
2	Quality Improvement Act of 1986, 42 U.S.C. § 11101–11152, and regulations
3	adopted to implement that act;
4	(8) information that originates from, or is intermingled so as to be
5	indistinguishable from, or that is treated in the same manner as information
6	described in subdivisions (2)–(7) of this subsection that a covered entity,
7	business associate, or a qualified service organization program creates,
8	collects, processes, uses, or maintains in the same manner as is required under
9	the laws, regulations, and guidelines described in subdivisions (2)–(7) of this
10	subsection;
11	(9) information processed or maintained solely in connection with, and
12	for the purpose of, enabling:
13	(A) an individual's employment or application for employment;
14	(B) an individual's ownership of, or function as a director or officer
15	of, a business entity;
16	(C) an individual's contractual relationship with a business entity;
17	(D) an individual's receipt of benefits from an employer, including
18	benefits for the individual's dependents or beneficiaries; or
19	(E) notice of an emergency to persons that an individual specifies;

H.121 Page 20 of 39

1	(10) any activity that involves collecting, maintaining, disclosing,
2	selling, communicating, or using information for the purpose of evaluating a
3	consumer's creditworthiness, credit standing, credit capacity, character,
4	general reputation, personal characteristics, or mode of living if done strictly in
5	accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C.
6	§ 1681–1681x, as may be amended, by:
7	(A) a consumer reporting agency;
8	(B) a person who furnishes information to a consumer reporting
9	agency under 15 U.S.C. § 1681s-2 (responsibilities of furnishers of
10	information to consumer reporting agencies); or
11	(C) a person who uses a consumer report as provided in 15 U.S.C.
12	§ 1681b(a)(3) (permissible purposes of consumer reports);
13	(11) information collected, processed, sold, or disclosed under and in
14	accordance with the following laws and regulations:
15	(A) the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721–
16	<u>2725;</u>
17	(B) the Family Educational Rights and Privacy Act, 20 U.S.C.
18	§ 1232g, and regulations adopted to implement that act;
19	(C) the Airline Deregulation Act, Pub. L. No. 95-504, only to the
20	extent that an air carrier collects information related to prices, routes, or

1	services, and only to the extent that the provisions of the Airline Deregulation
2	Act preempt this chapter;
3	(D) the Farm Credit Act, Pub. L. No. 92-181, as may be amended;
4	(E) federal policy under 21 U.S.C. § 830 (regulation of listed
5	chemicals and certain machines);
6	(12) nonpublic personal information that is processed by a financial
7	institution subject to the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, and
8	regulations adopted to implement that act;
9	(13) information that originates from, or is intermingled so as to be
10	indistinguishable from, information described in subdivision (12) of this
11	subsection and that a controller or processor collects, processes, uses, or
12	maintains in the same manner as is required under the law and regulations
13	specified in subdivision (12) of this subsection;
14	(14) a financial institution, credit union, independent trust company,
15	broker-dealer, or investment adviser or a financial institution's, credit union's.
16	independent trust company's, broker-dealer's, or investment adviser's affiliate
17	or subsidiary that is only and directly engaged in financial activities, as
18	described in 12 U.S.C. § 1843(k);
19	(15) a person regulated pursuant to 8 V.S.A. part 3 (chapters 101–165)
20	other than a person that, alone or in combination with another person,

1	establishes and maintains a self-insurance program and that does not otherwise
2	engage in the business of entering into policies of insurance;
3	(16) a third-party administrator, as that term is defined in the Third Party
4	Administrator Rule adopted pursuant to 18 V.S.A. § 9417;
5	(17) personal data of a victim or witness of child abuse, domestic
6	violence, human trafficking, sexual assault, violent felony, or stalking that a
7	victim services organization collects, processes, or maintains in the course of
8	its operation;
9	(18) a nonprofit organization that is established to detect and prevent
10	fraudulent acts in connection with insurance;
11	(19) information that is processed for purposes of compliance,
12	enrollment or degree verification, or research services by a nonprofit
13	organization that is established to provide enrollment data reporting services
14	on behalf of postsecondary schools as that term is defined in 16 V.S.A. § 176;
15	(20) noncommercial activity of:
16	(A) a publisher, editor, reporter, or other person who is connected
17	with or employed by a newspaper, magazine, periodical, newsletter, pamphlet,
18	report, or other publication in general circulation;
19	(B) a radio or television station that holds a license issued by the
20	Federal Communications Commission;

H.121 Page 23 of 39

1	(C) a nonprofit organization that provides programming to radio or
2	television networks; or
3	(D) an entity that provides an information service, including a press
4	association or wire service; or
5	(21) a public utility subject to the jurisdiction of the Public Utility
6	Commission under 30 V.S.A. § 203, but only until July 1, 2026.
7	Third: In Sec. 1, 9 V.S.A. chapter 61A, by striking out section 2427 in its
8	entirety and inserting in lieu thereof a new section 2427 to read as follows:
9	§ 2427. ENFORCEMENT; ATTORNEY GENERAL'S POWERS
10	(a) A person who violates this chapter or rules adopted pursuant to this
11	chapter commits an unfair and deceptive act in commerce in violation of
12	section 2453 of this title, provided that a private right of action under
13	subsection 2461(b) of this title shall not apply to the violation, and the
14	Attorney General shall have exclusive authority to enforce such violations.
15	(b) The Attorney General has the same authority to adopt rules to
16	implement the provisions of this section and to conduct civil investigations,
17	enter into assurances of discontinuance, bring civil actions, and take other
18	enforcement actions as provided under chapter 63, subchapter 1 of this title.
19	(c)(1) If the Attorney General determines that a violation of this chapter or
20	rules adopted pursuant to this chapter may be cured, the Attorney General may

H.121 Page 24 of 39

1	prior to initiating any action for the violation, issue a notice of violation
2	extending a 60-day cure period to the controller, processor, or consumer health
3	data controller alleged to have violated this chapter or rules adopted pursuant
4	to this chapter.
5	(2) The Attorney General may, in determining whether to grant a
6	controller, processor, or consumer health data controller the opportunity to
7	cure an alleged violation described in subdivision (1) of this subsection,
8	consider:
9	(A) the number of violations;
10	(B) the size and complexity of the controller, processor, or consumer
11	health data controller;
12	(C) the nature and extent of the controller's, processor's, or consume
13	health data controller's processing activities;
14	(D) the substantial likelihood of injury to the public;
15	(E) the safety of persons or property;
16	(F) whether the alleged violation was likely caused by human or
17	technical error; and
18	(G) the sensitivity of the data.
19	(d) Annually, on or before February 1, the Attorney General shall submit a
20	report to the General Assembly disclosing:

H.121 Page 25 of 39

1	(1) the number of notices of violation the Attorney General has issued;
2	(2) the nature of each violation;
3	(3) the number of violations that were cured during the available cure
4	period; and
5	(4) any other matter the Attorney General deems relevant for the
6	purposes of the report.
7	Fourth: In Sec. 7, 9 V.S.A. chapter 62, subchapter 6, in subdivision
8	2449a(10), following "designed or manipulated with the", by striking out the
9	word "substantial"
10	Fifth: By striking out Sec. 8, effective dates, in its entirety and inserting in
11	lieu thereof five new sections to be Secs. 8–12 to read as follows:
12	Sec. 8. STUDY; VERMONT DATA PRIVACY ACT
13	On or before January 15, 2026, the Attorney General shall review and report
14	their findings and recommendations to the House Committees on Commerce
15	and Economic Development, on Health Care, and on Judiciary and the Senate
16	Committees on Economic Development, Housing and General Affairs, on
17	Health and Welfare, and on Judiciary concerning policy recommendations for
18	improving data privacy in Vermont through:

H.121 Page 26 of 39

1	(1) development of legislative language for implementing a private right
2	of action in 9 V.S.A. chapter 61A, giving consideration to other state
3	approaches and including through structuring:
4	(A) violations giving rise to a private right of action in a manner that
5	addresses the gravest harms to consumers;
6	(B) applicability thresholds to ensure that the private right of action
7	does not harm good-faith actors or small Vermont businesses;
8	(C) damages that balance the consumer interest in enforcing the
9	consumer's personal data rights against the incentives a private right of action
10	may provide to litigants with frivolous claims; and
11	(D) other mechanisms to ensure the private right of action is targeted
12	to address persons engaging in unfair or deceptive acts;
13	(2) addressing the scope of health care exemptions under 9 V.S.A.
14	§ 2417(a)(2)–(8), including based on:
15	(I) research on the effects on the health care industry of the
16	health-related data-level exemptions under the Oregon Consumer Privacy Act;
17	(II) economic analysis of compliance costs for the health care
18	industry; and
19	(III) an analysis of health-related entities excluded from the
20	health care exemptions under 9 V.S.A. § 2417(a)(2)–(8); and

1	(3) analysis of the data security implications of implementation of the
2	Vermont Data Privacy Act.
3	Sec. 9. 9 V.S.A. § 2427 is amended to read:
4	§ 2427. ENFORCEMENT; ATTORNEY GENERAL'S POWERS
5	(a) A person who violates this chapter or rules adopted pursuant to this
6	chapter commits an unfair and deceptive act in commerce in violation of
7	section 2453 of this title, provided that a consumer private right of action under
8	subsection 2461(b) of this title shall not apply to the violation, and the
9	Attorney General shall have exclusive authority to enforce such violations
10	except as provided in subsection (d) of this section.
11	(b) The Attorney General has the same authority to adopt rules to
12	implement the provisions of this section and to conduct civil investigations,
13	enter into assurances of discontinuance, bring civil actions, and take other
14	enforcement actions as provided under chapter 63, subchapter 1 of this title.
15	(c)(1) If the Attorney General determines that a violation of this chapter or
16	rules adopted pursuant to this chapter may be cured, the Attorney General may,
17	prior to initiating any action for the violation, issue a notice of violation
18	extending a 60-day cure period to the controller, processor, or consumer health
19	data controller alleged to have violated this chapter or rules adopted pursuant
20	to this chapter.

1	(2) The Attorney General may, in determining whether to grant a
2	controller, processor, or consumer health data controller the opportunity to
3	cure an alleged violation described in subdivision (1) of this subsection,
4	consider:
5	(A) the number of violations;
6	(B) the size and complexity of the controller, processor, or consumer
7	health data controller;
8	(C) the nature and extent of the controller's, processor's, or consumer
9	health data controller's processing activities;
10	(D) the substantial likelihood of injury to the public;
11	(E) the safety of persons or property;
12	(F) whether the alleged violation was likely caused by human or
13	technical error; and
14	(G) the sensitivity of the data.
15	(d)(1) The private right of action available to a consumer for violations of
16	this chapter or rules adopted pursuant to this chapter shall be exclusively as
17	provided under this subsection.
18	(2) A consumer who is harmed by a data broker's or large data holder's
19	violation of subdivision 2419(b)(2) of this title, subdivision 2419(b)(3) of this
20	title, or section 2428 of this title may bring an action under subsection 2461(b)

1	of this title for the violation, but the right available under subsection 2461(b) of
2	this title shall not be available for a violation of any other provision of this
3	chapter or rules adopted pursuant to this chapter.
4	(e) Annually, on or before February 1, the Attorney General shall submit a
5	report to the General Assembly disclosing:
6	(1) the number of notices of violation the Attorney General has issued;
7	(2) the nature of each violation;
8	(3) the number of violations that were cured during the available cure
9	period; and
10	(4) the number of actions brought under subsection (d) of this section;
11	(5) the proportion of actions brought under subsection (d) of this section
12	that proceed to trial;
13	(6) the data brokers or large data holders most frequently sued under
14	subsection (d) of this section; and
15	(4)(7) any other matter the Attorney General deems relevant for the
16	purposes of the report.
17	Sec. 10. 9 V.S.A. § 2427 is amended to read:
18	§ 2427. ENFORCEMENT; ATTORNEY GENERAL'S POWERS
19	(a) A person who violates this chapter or rules adopted pursuant to this
20	chapter commits an unfair and deceptive act in commerce in violation of

(A) the number of violations;

19

1	section 2453 of this title, <u>provided that a consumer private right of action under</u>
2	subsection 2461(b) of this title shall not apply to the violation, and the
3	Attorney General shall have exclusive authority to enforce such violations
4	except as provided in subsection (d) of this section.
5	(b) The Attorney General has the same authority to adopt rules to
6	implement the provisions of this section and to conduct civil investigations,
7	enter into assurances of discontinuance, bring civil actions, and take other
8	enforcement actions as provided under chapter 63, subchapter 1 of this title.
9	(c)(1) If the Attorney General determines that a violation of this chapter or
10	rules adopted pursuant to this chapter may be cured, the Attorney General may,
11	prior to initiating any action for the violation, issue a notice of violation
12	extending a 60-day cure period to the controller, processor, or consumer health
13	data controller alleged to have violated this chapter or rules adopted pursuant
14	to this chapter.
15	(2) The Attorney General may, in determining whether to grant a
16	controller, processor, or consumer health data controller the opportunity to
17	cure an alleged violation described in subdivision (1) of this subsection,
18	consider:

1	(B) the size and complexity of the controller, processor, or consumer
2	health data controller;
3	(C) the nature and extent of the controller's, processor's, or consumer
4	health data controller's processing activities;
5	(D) the substantial likelihood of injury to the public;
6	(E) the safety of persons or property;
7	(F) whether the alleged violation was likely caused by human or
8	technical error; and
9	(G) the sensitivity of the data.
10	(d)(1) The private right of action available to a consumer for violations of
11	this chapter or rules adopted pursuant to this chapter shall be exclusively as
12	provided under this subsection.
13	(2) A consumer who is harmed by a data broker's or large data holder's
14	violation of subdivision 2419(b)(2) of this title, subdivision 2419(b)(3) of this
15	title, or section 2428 of this title may bring an action under subsection 2461(b)
16	of this title for the violation, but the right available under subsection 2461(b) of
17	this title shall not be available for a violation of any other provision of this
18	chapter or rules adopted pursuant to this chapter.
19	(e) Annually, on or before February 1, the Attorney General shall submit a
20	report to the General Assembly disclosing:

1	(1) the number of notices of violation the Attorney General has issued;
2	(2) the nature of each violation;
3	(3) the number of violations that were cured during the available cure
4	period; and
5	(4) the number of actions brought under subsection (d) of this section;
6	(5) the proportion of actions brought under subsection (d) of this section
7	that proceed to trial;
8	(6) the data brokers or large data holders most frequently sued under
9	subsection (d) of this section; and
10	(7) any other matter the Attorney General deems relevant for the
11	purposes of the report.
12	Sec. 11. 9 V.S.A. § 2417(a) is amended to read:
13	(a) This chapter does not apply to:
14	(1) a federal, State, tribal, or local government entity in the ordinary
15	course of its operation;
16	(2) a covered entity that is not a hybrid entity, any health care
17	component of a hybrid entity, or a business associate;
18	(3) information used only for public health activities and purposes
19	described in 45 C.F.R. § 164.512 (disclosure of protected health information
20	without authorization);

1	(4) 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) research on human subjects undertaken in accordance with good
6	clinical practice guidelines issued by the International Council for
7	Harmonisation of Technical Requirements for Pharmaceuticals for Human
8	Use;
9	(C) activities that are subject to the protections provided in 21 C.F.R.
10	Parts 50 (FDA clinical investigations protection of human subjects) and
11	56 (FDA clinical investigations institutional review boards); or
12	(D) research conducted in accordance with the requirements set forth
13	in subdivisions (A) through (C) of this subdivision (a)(4) or otherwise in
14	accordance with applicable law;
15	(5) patient identifying information that is collected and processed in
16	accordance with 42 C.F.R. Part 2 (confidentiality of substance use disorder
17	patient records);
18	(6) patient safety work product that is created for purposes of improving
19	patient safety under 42 C.F.R. Part 3 (patient safety organizations and patient
20	safety work product);

1	(7) information or documents created for the purposes of the Healthcare
2	Quality Improvement Act of 1986, 42 U.S.C. § 11101–11152, and regulations
3	adopted to implement that act;
4	(8) information that originates from, or is intermingled so as to be
5	indistinguishable from, or that is treated in the same manner as information
6	described in subdivisions (2)–(7) of this subsection that a covered entity,
7	business associate, or a qualified service organization program creates,
8	collects, processes, uses, or maintains in the same manner as is required under
9	the laws, regulations, and guidelines described in subdivisions (2)–(7) of this
10	subsection;
11	(9) information processed or maintained solely in connection with, and
12	for the purpose of, enabling:
13	(A) an individual's employment or application for employment;
14	(B) an individual's ownership of, or function as a director or officer
15	of, a business entity;
16	(C) an individual's contractual relationship with a business entity;
17	(D) an individual's receipt of benefits from an employer, including
18	benefits for the individual's dependents or beneficiaries; or
19	(E) notice of an emergency to persons that an individual specifies;

1	(10) any activity that involves collecting, maintaining, disclosing,
2	selling, communicating, or using information for the purpose of evaluating a
3	consumer's creditworthiness, credit standing, credit capacity, character,
4	general reputation, personal characteristics, or mode of living if done strictly in
5	accordance with the provisions of the Fair Credit Reporting Act, 15 U.S.C.
6	§ 1681–1681x, as may be amended, by:
7	(A) a consumer reporting agency;
8	(B) a person who furnishes information to a consumer reporting
9	agency under 15 U.S.C. § 1681s-2 (responsibilities of furnishers of
10	information to consumer reporting agencies); or
11	(C) a person who uses a consumer report as provided in 15 U.S.C.
12	§ 1681b(a)(3) (permissible purposes of consumer reports);
13	(11) information collected, processed, sold, or disclosed under and in
14	accordance with the following laws and regulations:
15	(A) the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721–
16	2725;
17	(B) the Family Educational Rights and Privacy Act, 20 U.S.C.
18	§ 1232g, and regulations adopted to implement that act;
19	(C) the Airline Deregulation Act, Pub. L. No. 95-504, only to the
20	extent that an air carrier collects information related to prices, routes, or

1	services, and only to the extent that the provisions of the Airline Deregulation
2	Act preempt this chapter;
3	(D) the Farm Credit Act, Pub. L. No. 92-181, as may be amended;
4	(E) federal policy under 21 U.S.C. § 830 (regulation of listed
5	chemicals and certain machines);
6	(12) nonpublic personal information that is processed by a financial
7	institution subject to the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, and
8	regulations adopted to implement that act;
9	(13) information that originates from, or is intermingled so as to be
10	indistinguishable from, information described in subdivision (12) of this
11	subsection and that a controller or processor collects, processes, uses, or
12	maintains in the same manner as is required under the law and regulations
13	specified in subdivision (12) of this subsection;
14	(14) a financial institution, credit union, independent trust company,
15	broker-dealer, or investment adviser or a financial institution's, credit union's
16	independent trust company's, broker-dealer's, or investment adviser's affiliate
17	or subsidiary that is only and directly engaged in financial activities, as
18	described in 12 U.S.C. § 1843(k);
19	(15) a person regulated pursuant to 8 V.S.A. part 3 (chapters 101–165)
20	other than a person that, alone or in combination with another person.

1	establishes and maintains a self-insurance program and that does not otherwise
2	engage in the business of entering into policies of insurance;
3	(16) a third-party administrator, as that term is defined in the Third Party
4	Administrator Rule adopted pursuant to 18 V.S.A. § 9417;
5	(17) personal data of a victim or witness of child abuse, domestic
6	violence, human trafficking, sexual assault, violent felony, or stalking that a
7	victim services organization collects, processes, or maintains in the course of
8	its operation;
9	(18) a nonprofit organization that is established to detect and prevent
10	fraudulent acts in connection with insurance;
11	(19) information that is processed for purposes of compliance,
12	enrollment or degree verification, or research services by a nonprofit
13	organization that is established to provide enrollment data reporting services
14	on behalf of postsecondary schools as that term is defined in 16 V.S.A. § 176;
15	<u>or</u>
16	(20) noncommercial activity of:
17	(A) a publisher, editor, reporter, or other person who is connected
18	with or employed by a newspaper, magazine, periodical, newsletter, pamphlet,
19	report, or other publication in general circulation;

H.121 Page 38 of 39

1	(B) a radio or television station that holds a license issued by the
2	Federal Communications Commission;
3	(C) a nonprofit organization that provides programming to radio or
4	television networks; or
5	(D) an entity that provides an information service, including a press
6	association or wire service; or
7	(21) a public utility subject to the jurisdiction of the Public Utility
8	Commission under 30 V.S.A. § 203, but only until July 1, 2026.
9	Sec. 12. EFFECTIVE DATES
10	(a) This section and Secs. 2 (public education and outreach), 3 (protection
11	of personal information), 4 (data broker opt-out study), and 8 (study; Vermont
12	Data Privacy Act) shall take effect on July 1, 2024.
13	(b) Secs. 1 (Vermont Data Privacy Act) and 7 (Age-Appropriate Design
14	Code) shall take effect on July 1, 2025.
15	(c) Secs. 5 (Vermont Data Privacy Act middle applicability threshold) and
16	11 (utilities exemption repeal) shall take effect on July 1, 2026.
17	(d) Sec. 9 (private right of action) shall take effect on January 1, 2027.
18	(e) Sec. 6 (Vermont Data Privacy Act low applicability threshold) shall
19	take effect on July 1, 2027.

H.121 Page 39 of 39

- 1 (f) Sec. 10 (private right of action repeal) shall take effect on January 1,
- 2 <u>2029.</u>