TO THE HOUSE OF REPRESENTATIVES:

The Committee on Commerce and Economic Development to which was referred Senate Bill No. 289 entitled "An act relating to age-appropriate design code" respectfully reports that it has considered the same and recommends that the House propose to the Senate that the bill be amended by striking out all after the enacting clause and inserting in lieu thereof the following:

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

CHAPTER 61A. VERMONT DATA PRIVACY ACT

§ 2415. DEFINITIONS

As used in this chapter:

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

(B) As used in subdivision (A) of this subdivision (1), "control" or "controlled" means:

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

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

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

(2) "Age estimation" means a process that estimates that a consumer is likely to be of a certain age, fall within an age range, or is over or under a certain age.

(A) Age estimation methods include:

(i) analysis of behavioral and environmental data the controller already collects about its consumers;

(ii) comparing the way a consumer interacts with a device or with consumers of the same age;

(iii) metrics derived from motion analysis; and

(iv) testing a consumer's capacity or knowledge.

(B) Age estimation does not require certainty, and if a controller estimates a consumer's age for the purpose of advertising or marketing, that estimation may also be used to comply with this chapter.

(3) "Age verification" means a system that relies on hard identifiers or verified sources of identification to confirm a consumer has reached a certain age, including government-issued identification or a credit card.

(4) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under subdivisions 2418(a)(1)–(5) of this title is being made by, or on behalf of, the consumer who is entitled to exercise the consumer rights with respect to the personal data at issue.

(5)(A) "Biometric data" means data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual, including:

(i) iris or retina scans;

(ii) fingerprints;

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

(iv) vein patterns;

(v) voice prints; and

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

(B) "Biometric data" does not include:

(i) a digital or physical photograph;

(ii) an audio or video recording; or

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

(6) "Broker-dealer" has the same meaning as in 9 V.S.A. § 5102.

(7) "Business associate" has the same meaning as in HIPAA.

(8) "Child" has the same meaning as in COPPA.

(9)(A) "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer.

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

(C) "Consent" does not include:

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

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

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

(10)(A) "Consumer" means an individual who is a resident of the State.

(B) "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit, or government agency.

(11) "Consumer health data" means any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, including gender-affirming health data and reproductive or sexual health data.

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

(13) "Consumer reporting agency" has the same meaning as in the Fair Credit Reporting Act, 15 U.S.C. § 1681a(f);

(14) "Controller" means a person who, alone or jointly with others, determines the purpose and means of processing personal data.

(15) "COPPA" means the Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501–6506, and any regulations, rules, guidance, and exemptions promulgated pursuant to the act, as the act and regulations, rules, guidance, and exemptions may be amended.

(16) "Covered entity" has the same meaning as in HIPAA.

(17) "Credit union" has the same meaning as in 8 V.S.A. § 30101.

(18) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice and includes any practice the Federal Trade Commission refers to as a "dark pattern."

(19) "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions made by the controller that result in the provision or denial by the controller of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice,

employment opportunities, health care services, or access to essential goods or services.

(20) "De-identified data" means data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to the individual, if the controller that possesses the data:

(A)(i) takes reasonable measures to ensure that the data cannot be used to re-identify an identified or identifiable individual or be associated with an individual or device that identifies or is linked or reasonably linkable to an individual or household;

(ii) for purposes of this subdivision (A), "reasonable measures" shall include the de-identification requirements set forth under 45 C.F.R. § 164.514 (other requirements relating to uses and disclosures of protected health information);

(B) publicly commits to process the data only in a de-identified fashion and not attempt to re-identify the data; and

(C) contractually obligates any recipients of the data to satisfy the criteria set forth in subdivisions (A) and (B) of this subdivision (20).

(21) "Financial institution":

(A) as used in subdivision 2417(a)(12) of this title, has the same meaning as in 15 U.S.C. § 6809; and

(B) as used in subdivision 2417(a)(14) of this title, has the same meaning as in 8 V.S.A. § 11101.

(22) "Gender-affirming health care services" has the same meaning as in 1 V.S.A. § 150.

(23) "Gender-affirming health data" means any personal data concerning a past, present, or future effort made by a consumer to seek, or a consumer's receipt of, gender-affirming health care services, including:

(A) precise geolocation data that is used for determining a consumer's attempt to acquire or receive gender-affirming health care services;

(B) efforts to research or obtain gender-affirming health care services; and

(C) any gender-affirming health data that is derived from nonhealth information.

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

(25) "Geofence" means any technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wireless fidelity technology data, or any other form of location detection, or any combination of such coordinates, connectivity, data, identification, or other form of location detection, to establish a virtual boundary.

(26) "Health care facility" has the same meaning as in 18 V.S.A. § 9432.

(27) "Heightened risk of harm to a minor" means processing the personal data of a minor in a manner that presents a reasonably foreseeable risk of:

(A) unfair or deceptive treatment of, or unlawful disparate impact on, a minor;

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

(C) unintended disclosure of the personal data of a minor; or

(D) any physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of a minor if the intrusion would be offensive to a reasonable person.

(28) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and any regulations promulgated pursuant to the act, as may be amended.

(29) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly, including by reference to an identifier such as a name, an identification number, specific geolocation data, or an online identifier.

(30) "Independent trust company" has the same meaning as in 8 V.S.A. § 2401.

(31) "Investment adviser" has the same meaning as in 9 V.S.A. § 5102.

(32) "Mental health facility" means any health care facility in which at least 70 percent of the health care services provided in the facility are mental health services.

(33) "Nonpublic personal information" has the same meaning as in 15 U.S.C. § 6809.

(34)(A) "Online service, product, or feature" means any service, product, or feature that is provided online, except as provided in subdivision (B) of this subdivision (34).

(B) "Online service, product, or feature" does not include:

(i) telecommunications service, as that term is defined in the Communications Act of 1934, 47 U.S.C. § 153;

(ii) broadband internet access service, as that term is defined in 47 C.F.R. § 54.400 (universal service support); or

(iii) the delivery or use of a physical product.

(35) "Patient identifying information" has the same meaning as in 42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).

(36) "Patient safety work product" has the same meaning as in 42 C.F.R. § 3.20 (patient safety organizations and patient safety work product).

(37)(A) "Personal data" means any information, including derived data and unique identifiers, that is linked or reasonably linkable to an identified or identifiable individual or to a device that identifies, is linked to, or is reasonably linkable to one or more identified or identifiable individuals in a household.

(B) "Personal data" does not include de-identified data or publicly available information.

(38)(A) "Precise geolocation data" means information derived from technology that can precisely and accurately identify the specific location of a consumer within a radius of 1,850 feet.

(B) "Precise geolocation data" does not include:

(i) the content of communications;

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

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

(39) "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets

of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(40) "Processor" means a person who processes personal data on behalf of a controller.

(41) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(42) "Protected health information" has the same meaning as in HIPAA.

(43) "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, provided the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(44)(A) "Publicly available information" means information that:

(i) is lawfully made available through federal, state, or local government records; or

(ii) a controller has a reasonable basis to believe that the consumer has lawfully made available to the general public through widely distributed media.

(B) "Publicly available information" does not include biometric data collected by a business about a consumer without the consumer's knowledge.

(45) "Qualified service organization" has the same meaning as in 42 C.F.R. § 2.11 (confidentiality of substance use disorder patient records).

(46) "Reproductive or sexual health care" has the same meaning as "reproductive health care services" in 1 V.S.A. § 150(c)(1).

(47) "Reproductive or sexual health data" means any personal data concerning a past, present, or future effort made by a consumer to seek, or a consumer's receipt of, reproductive or sexual health care.

(48) "Reproductive or sexual health facility" means any health care facility in which at least 70 percent of the health care-related services or products rendered or provided in the facility are reproductive or sexual health care.

(49)(A) "Sale of personal data" means the exchange of a consumer's personal data by the controller to a third party for monetary or other valuable consideration or otherwise for a commercial purpose.

(B) As used in this subdivision (49), "commercial purpose" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

(C) "Sale of personal data" does not include:

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

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

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

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

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

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

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

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

(50) "Sensitive data" means personal data that:

(A) reveals a consumer's government-issued identifier, such as a Social Security number, passport number, state identification card, or driver's license number, that is not required by law to be publicly displayed;

(B) reveals a consumer's racial or ethnic origin, national origin, citizenship or immigration status, religious or philosophical beliefs, or union membership;

(C) reveals a consumer's sexual orientation, sex life, sexuality, or status as transgender or nonbinary;

(D) reveals a consumer's status as a victim of a crime;

(E) is financial information, including a consumer's tax return and account number, financial account log-in, financial account, debit card number, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;

(F) is consumer health data;

(G) is personal data collected and analyzed concerning consumer health data or personal data that describes or reveals a past, present, or future mental or physical health condition, treatment, disability, or diagnosis, including pregnancy, to the extent the personal data is not used by the controller to identify a specific consumer's physical or mental health condition or diagnosis;

(H) is biometric or genetic data;

(I) is personal data collected from a known minor; or

(J) is precise geolocation data.

(51)(A) "Targeted advertising" means the targeting of an advertisement to a consumer based on the consumer's activity with one or more businesses, distinctly branded websites, applications, or services, other than the controller, distinctly branded website, application, or service with which the consumer is intentionally interacting.

(B) "Targeted advertising" does not include:

(i) an advertisement based on activities within the controller's own commonly branded website or online application;

(ii) an advertisement based on the context of a consumer's current search query, visit to a website, or use of an online application;

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

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

(52) "Third party" means a person, such as a public authority, agency, or body, other than the consumer, controller, or processor or an affiliate of the processor or the controller.

(53) "Trade secret" has the same meaning as in section 4601 of this title.

(54) "Victim services organization" means a nonprofit organization that is established to provide services to victims or witnesses of child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking.

§ 2416. APPLICABILITY

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

(1) controlled or processed the personal data of not fewer than 25,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

(2) controlled or processed the personal data of not fewer than 12,500 consumers and derived more than 25 percent of the person's gross revenue from the sale of personal data.

(b) Sections 2420, 2424, and 2428 of this title and the provisions of this chapter concerning consumer health data and consumer health data controllers apply to a person that conducts business in this State or a person that produces products or services that are targeted to residents of this State.

§ 2417. EXEMPTIONS

(a) This chapter does not apply to:

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

(2) protected health information that a covered entity or business associate processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with HIPAA;

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

(4) information that identifies a consumer in connection with:

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

(B) research on human subjects undertaken in accordance with good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

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

(D) research conducted in accordance with the requirements set forth in subdivisions (A) through (C) of this subdivision (a)(4) or otherwise in accordance with applicable law;

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

(6) patient safety work product that is created for purposes of improving patient safety under 42 C.F.R. Part 3 (patient safety organizations and patient safety work product);

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

(8) information that originates from, or is intermingled so as to be indistinguishable from, or that is treated in the same manner as information described in subdivisions (2)–(7) of this subsection that a covered entity, business associate, or a qualified service organization program creates, collects, processes, uses, or maintains in the same manner as is required under the laws, regulations, and guidelines described in subdivisions (2)–(7) of this subsection;

(9) information processed or maintained solely in connection with, and for the purpose of, enabling:

(A) an individual's employment or application for employment;

(B) an individual's ownership of, or function as a director or officer of, a business entity;

(C) an individual's contractual relationship with a business entity;

(D) an individual's receipt of benefits from an employer, including benefits for the individual's dependents or beneficiaries; or

(E) notice of an emergency to persons that an individual specifies;

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

(A) a consumer reporting agency;

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

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

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

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

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

(C) the Airline Deregulation Act, Pub. L. No. 95-504, only to the extent that an air carrier collects information related to prices, routes, or services, and only to the extent that the provisions of the Airline Deregulation Act preempt this chapter;

(D) the Farm Credit Act, Pub. L. No. 92-181, as may be amended;

(E) federal policy under 21 U.S.C. § 830 (regulation of listed chemicals and certain machines);

(12) nonpublic personal information that is processed by a financial institution subject to the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, and regulations adopted to implement that act;

(13) information that originates from, or is intermingled so as to be indistinguishable from, information described in subdivision (12) of this subsection and that a controller or processor collects, processes, uses, or maintains in the same manner as is required under the law and regulations specified in subdivision (12) of this subsection;

(14) a financial institution, credit union, independent trust company, broker-dealer, or investment adviser or a financial institution's, credit union's,

independent trust company's, broker-dealer's, or investment adviser's affiliate or subsidiary that is only and directly engaged in financial activities, as described in 12 U.S.C. § 1843(k);

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

(16) a third-party administrator, as that term is defined in the Third Party Administrator Rule adopted pursuant to 18 V.S.A. § 9417;

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

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

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

(20) noncommercial activity of:

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

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

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

(D) an entity that provides an information service, including a press association or wire service.

(b) Controllers, processors, and consumer health data controllers that comply with the verifiable parental consent requirements of COPPA shall be deemed compliant with any obligation to obtain parental consent pursuant to this chapter, including pursuant to section 2420 of this title.

§ 2418. CONSUMER PERSONAL DATA RIGHTS

(a) A consumer shall have the right to:

(1) confirm whether a controller is processing the consumer's personal data and, if a controller is processing the consumer's personal data, access the personal data;

(2) obtain from a controller a list of third parties to which the controller has disclosed the consumer's personal data or, if the controller does not

maintain this information in a format specific to the consumer, a list of third parties to which the controller has disclosed personal data;

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

(4) delete personal data provided by, or obtained about, the consumer unless retention of the personal data is required by law;

(5) if the processing of personal data is done by automatic means, obtain a copy of the consumer's personal data processed by the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance; and

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

(A) targeted advertising;

(B) the sale of personal data; or

(C) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(b)(1) A consumer may exercise rights under this section by submitting a request to a controller using the method that the controller specifies in the privacy notice under section 2419 of this title.

(2) A controller shall not require a consumer to create an account for the purpose described in subdivision (1) of this subsection, but the controller may require the consumer to use an account the consumer previously created.

(3) A parent or legal guardian may exercise rights under this section on behalf of the parent's child or on behalf of a child for whom the guardian has legal responsibility. A guardian or conservator may exercise the rights under this section on behalf of a consumer that is subject to a guardianship, conservatorship, or other protective arrangement.

(4)(A) A consumer may designate another person to act on the consumer's behalf as the consumer's authorized agent for the purpose of exercising the consumer's rights under subdivision (a)(4) or (a)(6) of this section.

(B) The consumer may designate an authorized agent by means of an internet link, browser setting, browser extension, global device setting, or other technology that enables the consumer to exercise the consumer's rights under subdivision (a)(4) or (a)(6) of this section.

(c) Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer rights authorized pursuant to this chapter as follows:

(1)(A) A controller shall respond to the consumer without undue delay, but not later than 45 days after receipt of the request.

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

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

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

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

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

(4)(A) If a controller is unable to authenticate a request to exercise any of the rights afforded under subdivisions (a)(1)–(5) of this section using commercially reasonable efforts, the controller shall not be required to comply

with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right or rights until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the right or rights.

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

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

(5) A controller that has obtained personal data about a consumer from a source other than the consumer shall be deemed in compliance with a consumer's request to delete the data pursuant to subdivision (a)(4) of this section by:

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

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

(6) A controller may not condition the exercise of a right under this section through:

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

(B) the employment of any dark pattern.

(d) A controller shall establish a process by means of which a consumer may appeal the controller's refusal to take action on a request under subsection (b) of this section. The controller's process must:

(1) Allow a reasonable period of time after the consumer receives the controller's refusal within which to appeal.

(2) Be conspicuously available to the consumer.

(3) Be similar to the manner in which a consumer must submit a request under subsection (b) of this section.

(4) Require the controller to approve or deny the appeal within 45 days after the date on which the controller received the appeal and to notify the consumer in writing of the controller's decision and the reasons for the decision. If the controller denies the appeal, the notice must provide or specify

information that enables the consumer to contact the Attorney General to submit a complaint.

(e) Nothing in this section shall be construed to require a controller to reveal a trade secret.

§ 2419. DUTIES OF CONTROLLERS

(a) A controller shall:

(1) limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains;

(2) establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue;

(3) provide an effective mechanism for a consumer to revoke consent to the controller's processing of the consumer's personal data that is at least as easy as the mechanism by which the consumer provided the consumer's consent; and

(4) upon a consumer's revocation of consent to processing, cease to process the consumer's personal data as soon as practicable, but not later than 15 days after receiving the request.

(b) A controller shall not:

(1) process personal data for a purpose not disclosed in the privacy notice required under subsection (d) of this section unless:

(A) the controller obtains the consumer's consent; or

(B) the purpose is reasonably necessary to and compatible with a disclosed purpose;

(2) process sensitive data about a consumer without first obtaining the consumer's consent or, if the controller knows the consumer is a child, without processing the sensitive data in accordance with COPPA;

(3) sell sensitive data;

(4) discriminate or retaliate against a consumer who exercises a right provided to the consumer under this chapter or refuses to consent to the processing of personal data for a separate product or service, including by:

(A) denying goods or services;

(B) charging different prices or rates for goods or services; or

(C) providing a different level of quality or selection of goods or services to the consumer;

(5) process personal data in violation of State or federal laws that prohibit unlawful discrimination; or

(6)(A) except as provided in subdivision (B) of this subdivision (6), process a consumer's personal data in a manner that discriminates against individuals or otherwise makes unavailable the equal enjoyment of goods or

services on the basis of an individual's actual or perceived race, color, sex, sexual orientation or gender identity, physical or mental disability, religion, ancestry, or national origin;

(B) subdivision (A) of this subdivision (6) shall not apply to:

(i) a private establishment, as that term is used in 42 U.S.C. § 2000a(e) (prohibition against discrimination or segregation in places of public accommodation);

(ii) processing for the purpose of a controller's or processor's self-testing to prevent or mitigate unlawful discrimination; or

(iii) processing for the purpose of diversifying an applicant, participant, or consumer pool.

(c) Subsections (a) and (b) of this section shall not be construed to:

(1) require a controller to provide a good or service that requires personal data from a consumer that the controller does not collect or maintain; or

(2) prohibit a controller from offering a different price, rate, level of quality, or selection of goods or services to a consumer, including an offer for no fee or charge, in connection with a consumer's voluntary participation in a financial incentive program, such as a bona fide loyalty, rewards, premium features, discount, or club card program, provided that the controller may not transfer personal data to a third party as part of the program unless:

(A) the transfer is necessary to enable the third party to provide a benefit to which the consumer is entitled; or

(B)(i) the terms of the program clearly disclose that personal data will be transferred to the third party or to a category of third parties of which the third party belongs; and

(ii) the consumer consents to the transfer.

(d)(1) A controller shall provide to consumers a reasonably accessible, clear, and meaningful privacy notice that:

(A) lists the categories of personal data, including the categories of sensitive data, that the controller processes;

(B) describes the controller's purposes for processing the personal data;

(C) describes how a consumer may exercise the consumer's rights under this chapter, including how a consumer may appeal a controller's denial of a consumer's request under section 2418 of this title;

(D) lists all categories of personal data, including the categories of sensitive data, that the controller shares with third parties;

(E) describes all categories of third parties with which the controller shares personal data at a level of detail that enables the consumer to understand what type of entity each third party is and, to the extent possible, how each third party may process personal data;

(F) specifies an e-mail address or other online method by which a consumer can contact the controller that the controller actively monitors;

(G) identifies the controller, including any business name under which the controller registered with the Secretary of State and any assumed business name that the controller uses in this State;

(H) provides a clear and conspicuous description of any processing of personal data in which the controller engages for the purposes of targeted advertising, sale of personal data to third parties, or profiling the consumer in furtherance of decisions that produce legal or similarly significant effects concerning the consumer, and a procedure by which the consumer may opt out of this type of processing; and

(I) describes the method or methods the controller has established for a consumer to submit a request under subdivision 2418(b)(1) of this title.

(2) The privacy notice shall adhere to the accessibility and usability guidelines recommended under 42 U.S.C. chapter 126 (the Americans with Disabilities Act) and 29 U.S.C. 794d (section 508 of the Rehabilitation Act of 1973), including ensuring readability for individuals with disabilities across various screen resolutions and devices and employing design practices that facilitate easy comprehension and navigation for all users.

(e) The method or methods under subdivision (d)(1)(I) of this section for submitting a consumer's request to a controller must:

(1) take into account the ways in which consumers normally interact with the controller, the need for security and reliability in communications related to the request, and the controller's ability to authenticate the identity of the consumer that makes the request;

(2) provide a clear and conspicuous link to a website where the consumer or an authorized agent may opt out from a controller's processing of the consumer's personal data pursuant to subdivision 2418(a)(6) of this title or, solely if the controller does not have a capacity needed for linking to a webpage, provide another method the consumer can use to opt out; and

(3) allow a consumer or authorized agent to send a signal to the controller that indicates the consumer's preference to opt out of the sale of personal data or targeted advertising pursuant to subdivision 2418(a)(6) of this title by means of a platform, technology, or mechanism that:

(A) does not unfairly disadvantage another controller;

(B) does not use a default setting but instead requires the consumer or authorized agent to make an affirmative, voluntary, and unambiguous choice to opt out;

(C) is consumer friendly and easy for an average consumer to use;

(D) is as consistent as possible with similar platforms, technologies, or mechanisms required under federal or state laws or regulations; and

(E)(i) enables the controller to reasonably determine whether the consumer has made a legitimate request pursuant to subsection 2418(b) of this title to opt out pursuant to subdivision 2418(a)(6) of this title; and

(ii) for purposes of subdivision (i) of this subdivision (C), use of an internet protocol address to estimate the consumer's location shall be considered sufficient to accurately determine residency.

(f) If a consumer or authorized agent uses a method under subdivision (d)(1)(I) of this section to opt out of a controller's processing of the consumer's personal data pursuant to subdivision 2418(a)(6) of this title and the decision conflicts with a consumer's voluntary participation in a bona fide reward, club card, or loyalty program or a program that provides premium features or discounts in return for the consumer's consent to the controller's processing of the consumer's personal data, the controller may either comply with the request to opt out or notify the consumer of the conflict and ask the consumer to affirm that the consumer intends to withdraw from the bona fide reward, club card, or loyalty program or the program that provides premium features or discounts. If the consumer affirms that the consumer intends to withdraw, the controller shall comply with the request to opt out.

§ 2420. DUTIES OF CONTROLLERS TO MINORS

(a)(1) A controller that offers any online service, product, or feature to a consumer whom the controller knows or consciously avoids knowing is a

minor shall use reasonable care to avoid any heightened risk of harm to minors caused by the online service, product, or feature.

(2) In any action brought pursuant to section 2427 of this title, there is a rebuttable presumption that a controller used reasonable care as required under this section if the controller complied with this section.

(b) A controller that offers any online service, product, or feature to a consumer whom the controller knows or consciously avoids knowing is a minor shall not process the minor's personal data for longer than is reasonably necessary to provide the online service, product, or feature.

(c) A controller that offers any online service, product, or feature to a consumer whom the controller knows or consciously avoids knowing is a minor and who has consented under subdivision 2419(b)(2) of this title to the processing of precise geolocation data shall:

(1) collect the minor's precise geolocation data only as reasonably necessary for the controller to provide the online service, product, or feature; and

(2) provide to the minor a conspicuous signal indicating that the controller is collecting the minor's precise geolocation data and make the signal available to the minor for the entire duration of the collection of the minor's precise geolocation data.

§ 2421. DUTIES OF PROCESSORS

(a) A processor shall adhere to a controller's instructions and shall assist the controller in meeting the controller's obligations under this chapter. In assisting the controller, the processor must:

(1) enable the controller to respond to requests from consumers pursuant to subsection 2418(b) of this title by means that:

(A) take into account how the processor processes personal data and the information available to the processor; and

(B) use appropriate technical and organizational measures to the extent reasonably practicable;

(2) adopt administrative, technical, and physical safeguards that are reasonably designed to protect the security and confidentiality of the personal data the processor processes, taking into account how the processor processes the personal data and the information available to the processor; and

(3) provide information reasonably necessary for the controller to conduct and document data protection assessments.

(b) Processing by a processor must be governed by a contract between the controller and the processor. The contract must:

(1) be valid and binding on both parties;

(2) set forth clear instructions for processing data, the nature and purpose of the processing, the type of data that is subject to processing, and the duration of the processing;

(3) specify the rights and obligations of both parties with respect to the subject matter of the contract;

(4) ensure that each person that processes personal data is subject to a duty of confidentiality with respect to the personal data;

(5) require the processor to delete the personal data or return the personal data to the controller at the controller's direction or at the end of the provision of services, unless a law requires the processor to retain the personal data;

(6) require the processor to make available to the controller, at the controller's request, all information the controller needs to verify that the processor has complied with all obligations the processor has under this chapter;

(7) require the processor to enter into a subcontract with a person the processor engages to assist with processing personal data on the controller's behalf and in the subcontract require the subcontractor to meet the processor's obligations concerning personal data;

(8)(A) allow the controller, the controller's designee, or a qualified and independent person the processor engages, in accordance with an appropriate and accepted control standard, framework, or procedure, to assess the processor's policies and technical and organizational measures for complying with the processor's obligations under this chapter;

(B) require the processor to cooperate with the assessment; and

(C) at the controller's request, report the results of the assessment to the controller; and

(9) prohibit the processor from combining personal data obtained from the controller with personal data that the processor:

(A) receives from or on behalf of another controller or person; or

(B) collects from an individual.

(c) This section does not relieve a controller or processor from any liability that accrues under this chapter as a result of the controller's or processor's actions in processing personal data.

(d)(1) For purposes of determining obligations under this chapter, a person is a controller with respect to processing a set of personal data and is subject to an action under section 2427 of this title to punish a violation of this chapter, if the person:

(A) does not adhere to a controller's instructions to process the personal data; or

(B) begins at any point to determine the purposes and means for processing the personal data, alone or in concert with another person.

(2) A determination under this subsection is a fact-based determination that must take account of the context in which a set of personal data is processed.

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

§ 2422. DUTIES OF PROCESSORS TO MINORS

(a) A processor shall adhere to the instructions of a controller and shall:

(1) assist the controller in meeting the controller's obligations under sections 2420 and 2424 of this title, taking into account:

(A) the nature of the processing;

(B) the information available to the processor by appropriate technical and organizational measures; and

(C) whether the assistance is reasonably practicable and necessary to assist the controller in meeting its obligations; and

(2) provide any information that is necessary to enable the controller to conduct and document data protection assessments pursuant to section 2424 of this title.

(b) A contract between a controller and a processor must satisfy the requirements in subsection 2421(b) of this title.

(c) Nothing in this section shall be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship as described in sections 2420 and 2424 of this title.

(d) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person that is not limited in the person's processing of personal data pursuant to a controller's instructions, or that fails to adhere to the instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor is a controller with respect to the processing and may be subject to an enforcement action under section 2427 of this title.

§ 2423. DATA PROTECTION ASSESSMENTS FOR PROCESSING ACTIVITIES THAT PRESENT A HEIGHTENED RISK OF HARM TO A CONSUMER

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

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

(2) the sale of personal data;

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

(A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(B) financial, physical, or reputational injury to consumers;

(C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person; or

(D) other substantial injury to consumers; and

(4) the processing of sensitive data.

(b)(1) Data protection assessments conducted pursuant to subsection (a) of this section shall:

(A) identify the categories of personal data processed, the purposes for processing the personal data, and whether the personal data is being transferred to third parties; and

(B) identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks.

(2) The controller shall factor into any data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c)(1) The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General pursuant to section 2427 of this title, and the controller shall make the data protection assessment available to the Attorney General.

(2) The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in this chapter.

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

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

(d) A single data protection assessment may address a comparable set of processing operations that present a similar heightened risk of harm.

(e) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this

section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(f) Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2025, and are not retroactive.

(g) A controller shall retain for at least five years all data protection assessments the controller conducts under this section.

§ 2424. DATA PROTECTION ASSESSMENTS FOR ONLINE SERVICES, PRODUCTS, OR FEATURES OFFERED TO MINORS

(a) A controller that offers any online service, product, or feature to a consumer whom the controller knows or consciously avoids knowing is a minor shall conduct a data protection assessment for the online service product or feature:

(1) in a manner that is consistent with the requirements established in section 2423 of this title; and

(2) that addresses:

(A) the purpose of the online service, product, or feature;

(B) the categories of a minor's personal data that the online service, product, or feature processes;

(C) the purposes for which the controller processes a minor's personal data with respect to the online service, product, or feature; and

(D) any heightened risk of harm to a minor that is a reasonably foreseeable result of offering the online service, product, or feature to a minor.

(b) A controller that conducts a data protection assessment pursuant to subsection (a) of this section shall review the data protection assessment as necessary to account for any material change to the processing operations of the online service, product, or feature that is the subject of the data protection assessment.

(c) If a controller conducts a data protection assessment pursuant to subsection (a) of this section or a data protection assessment review pursuant to subsection (b) of this section and determines that the online service, product, or feature that is the subject of the assessment poses a heightened risk of harm to a minor, the controller shall establish and implement a plan to mitigate or eliminate the heightened risk.

(d)(1) The Attorney General may require that a controller disclose any data protection assessment pursuant to subsection (a) of this section that is relevant to an investigation conducted by the Attorney General pursuant to section 2427 of this title, and the controller shall make the data protection assessment available to the Attorney General.

(2) The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in this chapter.

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

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

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

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

(g) Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2025, and are not retroactive.

(h) A controller that conducts a data protection assessment pursuant to subsection (a) of this section shall maintain documentation concerning the data protection assessment for the longer of:

(1) three years after the date on which the processing operations cease; or

(2) the date the controller ceases offering the online service, product, or feature.

§ 2425. DE-IDENTIFIED OR PSEUDONYMOUS DATA

(a) A controller in possession of de-identified data shall:

(1) take reasonable measures to ensure that the data cannot be used to re-identify an identified or identifiable individual or be associated with an individual or device that identifies or is linked or reasonably linkable to an individual or household;

(2) publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and

(3) contractually obligate any recipients of the de-identified data to comply with the provisions of this chapter.

(b) This section does not prohibit a controller from attempting to re-identify de-identified data solely for the purpose of testing the controller's methods for de-identifying data.

(c) This chapter shall not be construed to require a controller or processor to:

(1) re-identify de-identified data; or

(2) maintain data in identifiable form, or collect, obtain, retain, or access any data or technology, in order to associate a consumer with personal data in

order to authenticate the consumer's request under subsection 2418(b) of this title; or

(3) comply with an authenticated consumer rights request if the controller:

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

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

(C) does not sell or otherwise voluntarily disclose the personal data to any third party, except as otherwise permitted in this section.

(d) The rights afforded under subdivisions 2418(a)(1)–(5) of this title shall not apply to pseudonymous data in cases where the controller is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

(e) A controller that discloses or transfers pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified

data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

§ 2426. CONSTRUCTION OF DUTIES OF CONTROLLERS AND PROCESSORS

(a) This chapter shall not be construed to restrict a controller's, processor's, or consumer health data controller's ability to:

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

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

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

(4) carry out obligations under a contract under subsection 2421(b) of this title for a federal or State agency or local unit of government;

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

(6) provide a product or service specifically requested by the consumer to whom the personal data pertains consistent with subdivision 2419(a)(1) of this title;

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

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

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

(10) prevent, detect, protect against, or respond to a network security or physical security incident, including an intrusion or trespass, medical alert, or fire alarm;

(11) prevent, detect, protect against, or respond to identity theft, fraud, harassment, malicious or deceptive activity, or any criminal activity targeted at or involving the controller or processor or its services, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for the action;

(12) assist another controller, processor, consumer health data controller, or third party with any of the obligations under this chapter; or

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

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

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

(b) The obligations imposed on controllers, processors, or consumer health data controllers under this chapter shall not restrict a controller's, processor's, or consumer health data controller's ability to collect, use, or retain data for internal use to:

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

(2) effectuate a product recall; or

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

(c)(1) The obligations imposed on controllers, processors, or consumer health data controllers under this chapter shall not apply where compliance by the controller, processor, or consumer health data controller with this chapter would violate an evidentiary privilege under the laws of this State.

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

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

(d)(1) A controller, processor, or consumer health data controller that discloses personal data to a processor or third-party controller pursuant to this chapter shall not be deemed to have violated this chapter if the processor or third-party controller that receives and processes the personal data violates this chapter, provided, at the time the disclosing controller, processor, or consumer health data controller disclosed the personal data, the disclosing controller, processor, or consumer health data controller did not have actual knowledge that the receiving processor or third-party controller would violate this chapter.

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

(e) This chapter shall not be construed to:

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

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

(B) under 12 V.S.A. § 1615; or

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

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

(A)(i) reasonably necessary and proportionate to the purposes listed in this section; or

(ii) in the case of sensitive data, strictly necessary to the purposes listed in this section; and

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

(2)(A) Personal data collected, used, or retained pursuant to subsection (b) of this section shall, where applicable, take into account the nature and purpose or purposes of the collection, use, or retention.

(B) Personal data collected, used, or retained pursuant to subsection (b) of this section shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of

the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

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

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

(i) This chapter shall not be construed to require a controller, processor, or consumer health data controller to implement an age-verification or age-gating system or otherwise affirmatively collect the age of consumers. A controller, processor, or consumer health data controller that chooses to conduct commercially reasonable age estimation to determine which consumers are minors is not liable for an erroneous age estimation.

§ 2427. ENFORCEMENT

(a) A person who violates this chapter or rules adopted pursuant to this chapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

(b) The Attorney General has the same authority to adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, bring civil actions, and take other enforcement actions as provided under chapter 63, subchapter 1 of this title.

(c)(1) If the Attorney General determines that a violation of this chapter or rules adopted pursuant to this chapter may be cured, the Attorney General may, prior to initiating any action for the violation, issue a notice of violation extending a 60-day cure period to the controller, processor, or consumer health data controller alleged to have violated this chapter or rules adopted pursuant to this chapter.

(2) The Attorney General may, in determining whether to grant a controller, processor, or consumer health data controller the opportunity to cure an alleged violation described in subdivision (1) of this subsection, consider:

(A) the number of violations;

(B) the size and complexity of the controller, processor, or consumer health data controller;

(C) the nature and extent of the controller's, processor's, or consumer health data controller's processing activities;

(D) the substantial likelihood of injury to the public;

(E) the safety of persons or property;

(F) whether the alleged violation was likely caused by human or technical error; and

(G) the sensitivity of the data.

(d) Annually, on or before February 1, the Attorney General shall submit a report to the General Assembly disclosing:

(1) the number of notices of violation the Attorney General has issued;

(2) the nature of each violation;

(3) the number of violations that were cured during the available cure period; and

(4) any other matter the Attorney General deems relevant for the purposes of the report.

§ 2428. CONFIDENTIALITY OF CONSUMER HEALTH DATA

Except as provided in subsections 2417(a) and (b) of this title and section 2426 of this title, no person shall:

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

(2) provide any processor with access to consumer health data unless the person and processor comply with section 2421 of this title; or

(3) use a geofence to establish a virtual boundary that is within 1,850 feet of any health care facility, including any mental health facility or

reproductive or sexual health facility, for the purpose of identifying, tracking, collecting data from, or sending any notification to a consumer regarding the consumer's consumer health data.

Sec. 2. PUBLIC EDUCATION AND OUTREACH; ATTORNEY GENERAL STUDY

(a) The Attorney General shall implement a comprehensive public education, outreach, and assistance program for controllers and processors as those terms are defined in 9 V.S.A. § 2415. The program shall focus on:

(1) the requirements and obligations of controllers and processors under the Vermont Data Privacy Act;

(2) data protection assessments under 9 V.S.A. § 2421;

(3) enhanced protections that apply to children, minors, sensitive data, or consumer health data as those terms are defined in 9 V.S.A. § 2415;

(4) a controller's obligations to law enforcement agencies and the Attorney General's office;

(5) methods for conducting data inventories; and

(6) any other matters the Attorney General deems appropriate.

(b) The Attorney General shall provide guidance to controllers for establishing data privacy notices and opt-out mechanisms, which may be in the form of templates.

(c) The Attorney General shall implement a comprehensive public education, outreach, and assistance program for consumers as that term is defined in 9 V.S.A. § 2415. The program shall focus on:

(1) the rights afforded consumers under the Vermont Data Privacy Act, including:

(A) the methods available for exercising data privacy rights; and

(B) the opt-out mechanism available to consumers;

(2) the obligations controllers have to consumers;

(3) different treatment of children, minors, and other consumers under the act, including the different consent mechanisms in place for children and other consumers;

(4) understanding a privacy notice provided under the Act;

(5) the different enforcement mechanisms available under the Act, including the consumer's private right of action; and

(6) any other matters the Attorney General deems appropriate.

(d) The Attorney General shall cooperate with states with comparable data privacy regimes to develop any outreach, assistance, and education programs, where appropriate.

(e) The Attorney General may have the assistance of the Vermont Law and Graduate School in developing education, outreach, and assistance programs under this section.

(f) On or before December 15, 2026, the Attorney General shall assess the effectiveness of the implementation of the Act and submit a report to the House Committee on Commerce and Economic Development and the Senate Committee on Economic Development, Housing and General Affairs with its findings and recommendations, including any proposed draft legislation to address issues that have arisen since implementation.

Sec. 3. 9 V.S.A. chapter 62 is amended to read:

CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

Subchapter 1. General Provisions

§ 2430. DEFINITIONS

As used in this chapter:

(1) "Biometric data" shall have the same meaning as in section 2415 of this title.

(2)(A) "Brokered personal information" means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties:

(i) name;

(ii) address;

(iii) date of birth;

(iv) place of birth;

(v) mother's maiden name;

(vi) ~~unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of~~ biometric data;

(vii) name or address of a member of the consumer's immediate family or household;

(viii) Social Security number or other government-issued identification number; or

(ix) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

(B) "Brokered personal information" does not include publicly available information to the extent that it is related to a consumer's business or profession.

~~(2)~~(3) "Business" means a controller, a consumer health data controller, a processor, or a commercial entity, including a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United

States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but does not include the State, a State agency, any political subdivision of the State, or a vendor acting solely on behalf of, and at the direction of, the State.

~~(3)~~(4) "Consumer" means an individual residing in this State.

(5) "Consumer health data controller" has the same meaning as in section 2415 of this title.

(6) "Controller" has the same meaning as in section 2415 of this title.

~~(4)~~(7)(A) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

(B) Examples of a direct relationship with a business include if the consumer is a past or present:

(i) customer, client, subscriber, user, or registered user of the business's goods or services;

(ii) employee, contractor, or agent of the business;

(iii) investor in the business; or

(iv) donor to the business.

(C) The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, do not qualify the business as a data broker:

(i) developing or maintaining third-party e-commerce or application platforms;

(ii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier;

(iii) providing publicly available information related to a consumer's business or profession; or

(iv) providing publicly available information via real-time or near-real-time alert services for health or safety purposes.

(D) The phrase "sells or licenses" does not include:

(i) a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or

(ii) a sale or license of data that is merely incidental to the business.

~~(5)~~(8)(A) "Data broker security breach" means an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information maintained by a data broker

when the brokered personal information is not encrypted, redacted, or protected by another method that renders the information unreadable or unusable by an unauthorized person.

(B) "Data broker security breach" does not include good faith but unauthorized acquisition of brokered personal information by an employee or agent of the data broker for a legitimate purpose of the data broker, provided that the brokered personal information is not used for a purpose unrelated to the data broker's business or subject to further unauthorized disclosure.

(C) In determining whether brokered personal information has been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data broker may consider the following factors, among others:

(i) indications that the brokered personal information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing brokered personal information;

(ii) indications that the brokered personal information has been downloaded or copied;

(iii) indications that the brokered personal information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(iv) that the brokered personal information has been made public.

~~(6)~~(9) "Data collector" means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with personally identifiable information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators.

~~(7)~~(10) "Encryption" means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

~~(8)~~(11) "License" means a grant of access to, or distribution of, data by one person to another in exchange for consideration. A use of data for the sole benefit of the data provider, where the data provider maintains control over the use of the data, is not a license.

~~(9)~~(12) "Login credentials" means a consumer's user name or e-mail address, in combination with a password or an answer to a security question, that together permit access to an online account.

~~(10)~~(13)(A) "Personally identifiable information" means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted,

redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons:

(i) a Social Security number;

(ii) a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;

(iii) a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords;

(iv) a password, personal identification number, or other access code for a financial account;

(v) ~~unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of~~ biometric data;

(vi) genetic information; and

(vii)(I) health records or records of a wellness program or similar program of health promotion or disease prevention;

(II) a health care professional's medical diagnosis or treatment of the consumer; or

(III) a health insurance policy number.

(B) "Personally identifiable information" does not mean publicly available information that is lawfully made available to the general public from federal, State, or local government records.

(14) "Processor" has the same meaning as in section 2415 of this title.

~~(11)~~(15) "Record" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

~~(12)~~(16) "Redaction" means the rendering of data so that the data are unreadable or are truncated so that ~~no~~ not more than the last four digits of the identification number are accessible as part of the data.

~~(13)~~(17)(A) "Security breach" means unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information or login credentials maintained by a data collector.

(B) "Security breach" does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the data collector for a legitimate purpose of the data

collector, provided that the personally identifiable information or login credentials are not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

(C) In determining whether personally identifiable information or login credentials have been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others:

(i) indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;

(ii) indications that the information has been downloaded or copied;

(iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

(iv) that the information has been made public.

* * *

Subchapter 2. ~~Security Breach Notice Act~~ Data Security Breaches

* * *

§ 2436. NOTICE OF DATA BROKER SECURITY BREACH

(a) Short title. This section shall be known as the Data Broker Security Breach Notice Act.

(b) Notice of breach.

(1) Except as otherwise provided in subsection (c) of this section, any data broker shall notify the consumer that there has been a data broker security breach following discovery or notification to the data broker of the breach. Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency, as provided in subdivisions (3) and (4) of this subsection, or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) A data broker shall provide notice of a breach to the Attorney General as follows:

(A)(i) The data broker shall notify the Attorney General of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within 14 business days, consistent with the legitimate needs of the law enforcement agency, as provided in subdivisions (3) and (4) of this subsection (b), after the data broker's discovery of the security breach or when the data broker provides notice to consumers pursuant to this section, whichever is sooner.

(ii) If the date of the breach is unknown at the time notice is sent to the Attorney General, the data broker shall send the Attorney General the date of the breach as soon as it is known.

(iii) Unless otherwise ordered by a court of this State for good cause shown, a notice provided under this subdivision (2)(A) shall not be disclosed to any person other than the authorized agent or representative of the Attorney General, a State's Attorney, or another law enforcement officer engaged in legitimate law enforcement activities without the consent of the data broker.

(B)(i) When the data broker provides notice of the breach pursuant to subdivision (1) of this subsection (b), the data broker shall notify the Attorney General of the number of Vermont consumers affected, if known to the data broker, and shall provide a copy of the notice provided to consumers under subdivision (1) of this subsection (b).

(ii) The data broker may send to the Attorney General a second copy of the consumer notice, from which is redacted the type of brokered personal information that was subject to the breach, that the Attorney General shall use for any public disclosure of the breach.

(3) The notice to a consumer required by this subsection shall be delayed upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law

enforcement investigation or a national or Homeland Security investigation or jeopardize public safety or national or Homeland Security interests. In the event law enforcement makes the request for a delay in a manner other than in writing, the data broker shall document the request contemporaneously in writing and include the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. A law enforcement agency shall promptly notify the data broker in writing when the law enforcement agency no longer believes that notification may impede a law enforcement investigation or a national or Homeland Security investigation, or jeopardize public safety or national or Homeland Security interests. The data broker shall provide notice required by this section without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay.

(4) The notice to a consumer required in subdivision (1) of this subsection shall be clear and conspicuous. A notice to a consumer of a security breach involving brokered personal information shall include a description of each of the following, if known to the data broker:

(A) the incident in general terms;

(B) the type of brokered personal information that was subject to the security breach;

(C) the general acts of the data broker to protect the brokered personal information from further security breach;

(D) a telephone number, toll-free if available, that the consumer may call for further information and assistance;

(E) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and

(F) the approximate date of the data broker security breach.

(5) A data broker may provide notice of a security breach involving brokered personal information to a consumer by two or more of the following methods:

(A) written notice mailed to the consumer's residence;

(B) electronic notice, for those consumers for whom the data broker has a valid e-mail address, if:

(i) the data broker's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or

(ii) the notice is consistent with the provisions regarding electronic records and signatures for notices in 15 U.S.C. § 7001;

(C) telephonic notice, provided that telephonic contact is made directly with each affected consumer and not through a prerecorded message; or

(D) notice by publication in a newspaper of statewide circulation in the event the data broker cannot effectuate notice by any other means.

(c) Exception.

(1) Notice of a security breach pursuant to subsection (b) of this section is not required if the data broker establishes that misuse of brokered personal information is not reasonably possible and the data broker provides notice of the determination that the misuse of the brokered personal information is not reasonably possible pursuant to the requirements of this subsection. If the data broker establishes that misuse of the brokered personal information is not reasonably possible, the data broker shall provide notice of its determination that misuse of the brokered personal information is not reasonably possible and a detailed explanation for said determination to the Vermont Attorney General. The data broker may designate its notice and detailed explanation to the Vermont Attorney General as a trade secret if the notice and detailed explanation meet the definition of trade secret contained in 1 V.S.A. § 317(c)(9).

(2) If a data broker established that misuse of brokered personal information was not reasonably possible under subdivision (1) of this

subsection and subsequently obtains facts indicating that misuse of the brokered personal information has occurred or is occurring, the data broker shall provide notice of the security breach pursuant to subsection (b) of this section.

(d) Waiver. Any waiver of the provisions of this subchapter is contrary to public policy and is void and unenforceable.

(e) Enforcement.

(1) With respect to a controller or processor other than a controller or processor licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of this chapter and to enforce, prosecute, obtain, and impose remedies for a violation of this chapter or any rules or regulations adopted pursuant to this chapter as the Attorney General and State's Attorney have under chapter 63 of this title. The Attorney General may refer the matter to the State's Attorney in an appropriate case. The Superior Courts shall have jurisdiction over any enforcement matter brought by the Attorney General or a State's Attorney under this subsection.

(2) With respect to a controller or processor that is licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Department of Financial Regulation shall have the full authority to investigate potential violations of this chapter and to enforce, prosecute, obtain, and

impose remedies for a violation of this chapter or any rules or regulations adopted pursuant to this chapter, as the Department has under Title 8 or this title or any other applicable law or regulation.

* * *

Subchapter 5. Data Brokers

§ 2446. DATA BROKERS; ANNUAL REGISTRATION

(a) Annually, on or before January 31 following a year in which a person meets the definition of data broker as provided in section 2430 of this title, a data broker shall:

(1) register with the Secretary of State;

(2) pay a registration fee of $100.00; and

(3) provide the following information:

(A) the name and primary physical, e-mail, and ~~Internet~~ internet addresses of the data broker;

(B) if the data broker permits a consumer to opt out of the data broker's collection of brokered personal information, opt out of its databases, or opt out of certain sales of data:

(i) the method for requesting an opt-out;

(ii) if the opt-out applies to only certain activities or sales, which ones; and

(iii) whether the data broker permits a consumer to authorize a third party to perform the opt-out on the consumer's behalf;

(C) a statement specifying the data collection, databases, or sales activities from which a consumer may not opt out;

(D) a statement whether the data broker implements a purchaser credentialing process;

(E) the number of data broker security breaches that the data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches;

(F) where the data broker has actual knowledge that it possesses the brokered personal information of minors, a separate statement detailing the data collection practices, databases, sales activities, and opt-out policies that are applicable to the brokered personal information of minors; and

(G) any additional information or explanation the data broker chooses to provide concerning its data collection practices.

(b) A data broker that fails to register pursuant to subsection (a) of this section is liable to the State for:

(1) a civil penalty of ~~$50.00~~ $125.00 for each day~~, not to exceed a total of $10,000.00 for each year,~~ it fails to register pursuant to this section;

(2) an amount equal to the fees due under this section during the period it failed to register pursuant to this section; and

(3) other penalties imposed by law.

(c) A data broker that omits required information from its registration shall file an amendment to include the omitted information within 30 business days following notification of the omission and is liable to the State for a civil penalty of $1,000.00 per day for each day thereafter.

(d) A data broker that files materially incorrect information in its registration:

(1) is liable to the State for a civil penalty of $25,000.00; and

(2) if it fails to correct the false information within 30 business days after discovery or notification of the incorrect information, an additional civil penalty of $1,000.00 per day for each day thereafter that it fails to correct the information.

(e) The Attorney General may maintain an action in the Civil Division of the Superior Court to collect the penalties imposed in this section and to seek appropriate injunctive relief.

* * *

§ 2448. DATA BROKERS; CREDENTIALING

(a) Credentialing.

(1) A data broker shall maintain reasonable procedures designed to ensure that the brokered personal information it discloses is used for a legitimate and legal purpose.

(2) These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information shall be used for no other purpose.

(3) A data broker shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by the prospective user prior to furnishing the user brokered personal information.

(4) A data broker shall not furnish brokered personal information to any person if it has reasonable grounds for believing that the brokered personal information will not be used for a legitimate and legal purpose.

Sec. 4. STUDY; DATA BROKERS; OPT OUT

On or before January 1, 2025, the Secretary of State, in collaboration with the Agency of Digital Services, the Attorney General, and interested parties, shall review and report their findings and recommendations to the House Committee on Commerce and Economic Development and the Senate Committee on Economic Development, Housing and General Affairs concerning one or more mechanisms for Vermont consumers to opt out of the collection, retention, and sale of brokered personal information, including:

(1) an individual opt out that requires a data broker to allow a consumer to opt out of its data collection, retention, and sales practices through a request made directly to the data broker; and

(2) specifically considering the rules, procedures, and framework for implementing the "accessible deletion mechanism" by the California Privacy Protection Agency that takes effect on January 1, 2026, and approaches in other jurisdictions if applicable:

(A) how to design and implement a State-facilitated general opt out mechanism;

(B) the associated implementation and operational costs;

(C) mitigation of security risks; and

(D) other relevant considerations.

Sec. 5. 9 V.S.A. § 2416(a) is amended to read:

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

(1) controlled or processed the personal data of not fewer than ~~25,000~~ 12,500 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

(2) controlled or processed the personal data of not fewer than ~~12,500~~ 6,250 consumers and derived more than ~~25~~ 20 percent of the person's gross revenue from the sale of personal data.

Sec. 6. 9 V.S.A. § 2416(a) is amended to read:

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

(1) controlled or processed the personal data of not fewer than ~~12,500~~ 6,250 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

(2) controlled or processed the personal data of not fewer than ~~6,250~~ 3,125 consumers and derived more than 20 percent of the person's gross revenue from the sale of personal data.

Sec. 7. 9 V.S.A. § 2427 is amended to read:

§ 2427. ENFORCEMENT

(a) A person who violates this chapter or rules adopted pursuant to this chapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

(b) The Attorney General has the same authority to adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, bring civil actions, and take other enforcement actions as provided under chapter 63, subchapter 1 of this title.

~~(c)(1) If the Attorney General determines that a violation of this chapter or rules adopted pursuant to this chapter may be cured, the Attorney General may, prior to initiating any action for the violation, issue a notice of violation extending a 60-day cure period to the controller, processor, or consumer health data controller alleged to have violated this chapter or rules adopted pursuant to this chapter.~~

~~(2) The Attorney General may, in determining whether to grant a controller, processor, or consumer health data controller the opportunity to cure an alleged violation described in subdivision (1) of this subsection, consider:~~

~~(A) the number of violations;~~

~~(B) the size and complexity of the controller, processor, or consumer health data controller;~~

~~(C) the nature and extent of the controller's, processor's, or consumer health data controller's processing activities;~~

~~(D) the substantial likelihood of injury to the public;~~

~~(E) the safety of persons or property;~~

~~(F) whether the alleged violation was likely caused by human or technical error; and~~

~~(G) the sensitivity of the data.~~

~~(d) Annually, on or before February 1, the Attorney General shall submit a report to the General Assembly disclosing:~~

~~(1) the number of notices of violation the Attorney General has issued;~~

~~(2) the nature of each violation;~~

~~(3) the number of violations that were cured during the available cure period; and~~

~~(4) any other matter the Attorney General deems relevant for the purposes of the report.~~

Sec. 8. 9 V.S.A. § 2427 is amended to read:

§ 2427. ENFORCEMENT AND PRIVATE RIGHT OF ACTION

(a) A person who violates this chapter or rules adopted pursuant to this chapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

(b) The Attorney General has the same authority to adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, bring civil actions, and take other enforcement actions as provided under chapter 63, subchapter 1 of this title.

(c)(1) A consumer who is harmed by a controller's, processor's, or consumer health data controller's violation of subdivision 2419(b)(2) of this title, subdivision 2419(b)(3) of this title, or section 2428 of this title may bring

an action in Superior Court against the controller, processor, or consumer health data controller for the alleged violation if:

(A) the consumer notifies the controller, processor, or consumer health data controller of the violation; and

(B)(i) the controller, processor, or consumer health data controller fails to cure the violation within 60 days following receipt of the notice of violation; or

(ii) no cure is possible.

(2) A consumer bringing an action under this subsection may seek:

(A) the greater of $1,000.00 or actual damages;

(B) injunctive relief;

(C) punitive damages in the case of an intentional violation; and

(D) reasonable costs and attorney's fees.

(d) Annually, on or before February 1, the Attorney General shall submit a report to the General Assembly disclosing:

(1) the number of actions brought under subsection (c) of this section;

(2) the number of violations asserted, broken down by statutory basis;

(3) the proportion of actions brought under subsection (c) of this section that proceed to trial;

(4) the controllers, processors, or consumer health data controllers most frequently sued under subsection (c) of this section; and

(5) any other matter the Attorney General deems relevant for the purposes of the report.

Sec. 9. 9 V.S.A. § 2427 is amended to read:

§ 2427. ENFORCEMENT ~~AND PRIVATE RIGHT OF ACTION~~

(a) A person who violates this chapter or rules adopted pursuant to this chapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

(b) The Attorney General has the same authority to adopt rules to implement the provisions of this section and to conduct civil investigations, enter into assurances of discontinuance, bring civil actions, and take other enforcement actions as provided under chapter 63, subchapter 1 of this title.

~~(c)(1) A consumer who is harmed by a controller's, processor's, or consumer health data controller's violation of subdivision 2419(b)(2) of this title, subdivision 2419(b)(3) of this title, or section 2428 of this title may bring an action in Superior Court against the controller, processor, or consumer health data controller for the alleged violation if:~~

~~(A) the consumer notifies the controller, processor, or consumer health data controller of the violation; and~~

~~(B)(i) the controller, processor, or consumer health data controller fails to cure the violation within 60 days following receipt of the notice of violation; or~~

~~(ii) no cure is possible.~~

~~(2) A consumer bringing an action under this subsection may seek:~~

~~(A) the greater of $1,000.00 or actual damages;~~

~~(B) injunctive relief;~~

~~(C) punitive damages in the case of an intentional violation; and~~

~~(D) reasonable costs and attorney's fees.~~

~~(d) Annually, on or before February 1, the Attorney General shall submit a report to the General Assembly disclosing:~~

~~(1) the number of actions brought under subsection (c) of this section;~~

~~(2) the number of violations asserted, broken down by statutory basis;~~

~~(3) the proportion of actions brought under subsection (c) of this section that proceed to trial;~~

~~(4) the controllers, processors, or consumer health data controllers most frequently sued under subsection (c) of this section; and~~

~~(5) any other matter the Attorney General deems relevant for the purposes of the report.~~

Sec. 10. 9 V.S.A. chapter 62, subchapter 6 is added to read:

Subchapter 6. Age-Appropriate Design Code

§ 2449a. DEFINITIONS

As used in this subchapter:

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

(B) As used in subdivision (A) of this subdivision (1), "control" or "controlled" means:

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

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

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

(2) "Age-appropriate" means a recognition of the distinct needs and diversities of minor consumers at different age ranges. In order to help support the design of online services, products, and features, covered businesses should take into account the unique needs and diversities of different age ranges, including the following developmental stages: zero to five years of age or "preliterate and early literacy"; six to nine years of age or "core primary school years"; 10 to 12 years of age or "transition years"; 13 to 15 years of age or "early teens"; and 16 to 17 years or age or "approaching adulthood."

(3) "Age estimation" means a process that estimates that a user is likely to be of a certain age, fall within an age range, or is over or under a certain age.

(A) Age estimation methods include:

(i) analysis of behavioral and environmental data the covered business already collects about its users;

(ii) comparing the way a user interacts with a device or with users of the same age;

(iii) metrics derived from motion analysis; and

(iv) testing a user's capacity or knowledge.

(B) Age estimation does not require certainty, and if a covered business estimates a user's age for the purpose of advertising or marketing, that estimation may also be used to comply with this act.

(4) "Age verification" means a system that relies on hard identifiers or verified sources of identification to confirm a user has reached a certain age, including government-issued identification or a credit card.

(5) "Business associate" has the same meaning as in HIPAA.

(6) "Collect" means buying, renting, gathering, obtaining, receiving, or accessing any personal data by any means. This includes receiving data from the consumer, either actively or passively, or by observing the consumer's behavior.

(7)(A) "Consumer" means an individual who is a Vermont resident.

(B) "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer,

or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency whose communications or transactions with the covered business occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit, or government agency.

(8) "Covered business" means a sole proprietorship, partnership, limited liability company, corporation, association, other legal entity, or an affiliate thereof, that conducts business in this State or that produces online products, services, or features that are targeted to residents of this State and that:

(A) collects consumers' personal data or has consumers' personal data collected on its behalf by a third party;

(B) alone or jointly with others determines the purposes and means of the processing of consumers personal data; and

(C) alone or in combination annually buys, receives for commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal data of at least 50 percent of its consumers.

(9) "Covered entity" has the same meaning as in HIPAA.

(10) "Dark pattern" means a user interface designed or manipulated with the effect of subverting or impairing user autonomy, decision making, or choice, and includes any practice the Federal Trade Commission categorizes as a "dark pattern."

(11) "Default" means a preselected option adopted by the covered business for the online service, product, or feature.

(12) "Deidentified" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable consumer, or a device linked to such consumer, provided that the covered business that possesses the data:

(A) takes reasonable measures to ensure that the data cannot be associated with a consumer;

(B) publicly commits to maintain and use the data only in a deidentified fashion and not attempt to reidentify the data; and

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

(13) "Derived data" means data that is created by the derivation of information, data, assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or another source of information or data about a minor consumer or a minor consumer's device.

(14)(A) "Low-friction variable reward" means a design feature or virtual item that intermittently rewards consumers for scrolling, tapping, opening, or continuing to engage in an online service, product, or feature.

(B) Examples of low-friction variable reward designs include endless scroll, auto play, and nudges meant to encourage reengagement.

(15)(A) "Minor consumer" means an individual under 18 years of age who is a Vermont resident.

(B) "Minor consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit, or government agency.

(16) "Online service, product, or feature" means a digital product that is accessible to the public via the internet, including a website or application, and does not mean any of the following:

(A) telecommunications service, as defined in 47 U.S.C. § 153;

(B) a broadband internet access service as defined in 47 C.F.R. § 54.400; or

(C) the sale, delivery, or use of a physical product.

(17) "Personal data" means any information, including derived data and unique identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or to a device that identifies, is linked to, or is reasonably linkable to one or more identified or identifiable individuals in a household. Personal data does not include deidentified data or publicly available information.

(18) "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, modification, or otherwise handling of personal data.

(19) "Processor" means a person who processes personal data on behalf of a covered business.

(20) "Profile" or "profiling" means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable consumer's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(21) "Publicly available information" means information that:

(A) is lawfully made available through federal, state, or local government records; or

(B) a covered business has a reasonable basis to believe that the consumer has lawfully made available to the general public through widely distributed media.

(22) "Reasonably likely to be accessed" means an online service, product, or feature that is likely to be accessed by minor consumers based on any of the following indicators:

(A) the online service, product, or feature is directed to children, as defined by the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 and the Federal Trade Commission rules implementing that Act;

(B) the online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by an audience that is composed of at least two percent minor consumers two through under 18 years of age;

(C) the online service, product, or feature contains advertisements marketed to minor consumers;

(D) the audience of the online service, product, or feature is determined, based on internal company research, to be composed of at least two percent minor consumers two through under 18 years of age; or

(E) the covered business knew or should have known that at least two percent of the audience of the online service, product, or feature includes minor consumers two through under 18 years of age, provided that, in making this assessment, the business shall not collect or process any personal data that is not reasonably necessary to provide an online service, product, or feature with which a minor consumer is actively and knowingly engaged.

(23)(A) "Social media platform" means a public or semi-public internet-based service or application that is primarily intended to connect and allow a

user to socially interact within such service or application and enables a user to:

(i) construct a public or semi-public profile for the purposes of signing into and using such service or application;

(ii) populate a public list of other users with whom the user shares a social connection within such service or application; or

(iii) create or post content that is viewable by other users, including content on message boards and in chat rooms, and that presents the user with content generated by other users.

(B) "Social media platform" does not mean a public or semi-public internet-based service or application that:

(i) exclusively provides electronic mail or direct messaging services;

(ii) primarily consists of news, sports, entertainment, interactive video games, electronic commerce, or content that is preselected by the provider for which any interactive functionality is incidental to, directly related to, or dependent on the provision of such content; or

(iii) is used by and under the direction of an educational entity, including a learning management system or a student engagement program.

(24) "Third party" means a natural or legal person, public authority, agency, or body other than the consumer or the covered business.

§ 2449b. EXCLUSIONS

This subchapter does not apply to:

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

(2) protected health information that a covered entity or business associate processes in accordance with, or documents that a covered entity or business associate creates for the purpose of complying with, HIPAA;

(3) information used only for public health activities and purposes described in 45 C.F.R. § 164.512;

(4) information that identifies a consumer in connection with:

(A) activities that are subject to the Federal Policy for the Protection of Human Subjects as set forth in 45 C.F.R. Part 46;

(B) research on human subjects undertaken in accordance with good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use;

(C) activities that are subject to the protections provided in 21 C.F.R. 50 and 21 C.F.R. Part 56; or

(D) research conducted in accordance with the requirements set forth in subdivisions (A)–(C) of this subdivision (4) or otherwise in accordance with State or federal law; and

(5) an entity whose primary purpose is journalism as defined in 12 V.S.A. § 1615(a)(2) and that has a majority of its workforce consisting of individuals engaging in journalism.

§ 2449c. MINIMUM DUTY OF CARE

(a) A covered business that processes a minor consumer's data in any capacity owes a minimum duty of care to the minor consumer.

(b) As used in this subchapter, "a minimum duty of care" means the use of the personal data of a minor consumer and the design of an online service, product, or feature will not benefit the covered business to the detriment of a minor consumer and will not result in:

(1) reasonably foreseeable emotional distress as defined in 13 V.S.A. § 1061(2) to a minor consumer;

(2) the encouragement of excessive or compulsive use of the online service, product, or feature by a minor consumer; or

(3) discrimination against the minor consumer based upon race, ethnicity, sex, disability, sexual orientation, gender identity, gender expression, or national origin.

§ 2449d. COVERED BUSINESS OBLIGATIONS

(a) A covered business that is reasonably likely to be accessed and subject to this subchapter shall:

(1) configure all default privacy settings provided to a minor consumer through the online service, product, or feature to a high level of privacy;

(2) provide privacy information, terms of service, policies, and community standards concisely and prominently;

(3) provide prominent, accessible, and responsive tools to help a minor consumer or, if applicable, their parents or guardians to exercise their privacy rights and report concerns to the covered business;

(4) honor the request of a minor consumer to unpublish the minor consumer's social media platform account not later than 15 business days after a covered business receives such a request from a minor consumer; and

(5) provide easily accessible and age-appropriate tools for a minor consumer to limit the ability of users or covered businesses to send unsolicited communications.

(b) A violation of this section constitutes a violation of the minimum duty of care as provided in section 2449c of this subchapter.

§ 2449e. COVERED BUSINESS PROHIBITIONS

(a) A covered business that is reasonably likely to be accessed and subject to this subchapter shall not:

(1) use low-friction variable reward design features that encourage excessive and compulsive use by a minor consumer;

(2) permit, by default, an unknown adult to contact a minor consumer on its platform without the minor consumer first initiating that contact;

(3) permit a minor consumer to be exploited by a contract on the online service, product, or feature;

(4) use dark patterns; or

(5) permit a parent or guardian of a minor consumer, or any other consumer, to monitor the online activity of a minor consumer or to track the location of the minor consumer without providing a conspicuous signal to the minor consumer when the minor consumer is being monitored or tracked.

(b) A violation of this section constitutes a violation of the minimum duty of care as provided in section 2449c of this subchapter.

§ 2449f. ATTORNEY GENERAL ENFORCEMENT

(a) A covered business that violates this subchapter or rules adopted pursuant to this subchapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

(b) The Attorney General shall have the same authority under this subchapter to make rules, conduct civil investigations, bring civil actions, and enter into assurances of discontinuance as provided under chapter 63 of this title.

§ 2449g. LIMITATIONS

Nothing in this subchapter shall be interpreted or construed to:

(1) Impose liability in a manner that is inconsistent with 47 U.S.C. § 230.

(2) Prevent or preclude any minor consumer from deliberately or independently searching for, or specifically requesting, content.

(3) Require a covered business to implement an age verification requirement. The obligations imposed under this act should be done with age estimation techniques and do not require age verification.

§ 2449h. RIGHTS AND FREEDOMS OF MINOR CONSUMERS

It is the intent of the General Assembly that nothing in this act may be construed to infringe on the existing rights and freedoms of minor consumers or be construed to discriminate against the minor consumer based on race, ethnicity, sex, disability, sexual orientation, gender identity, gender expression, or national origin.

Sec. 11. EFFECTIVE DATES

(a) This section and Secs. 2 (public education and outreach), 3 (protection of personal information), and 4 (data broker opt-out study) shall take effect on July 1, 2024.

(b) Secs. 1 (Vermont Data Privacy Act) and 10 (Age-Appropriate Design Code) shall take effect on July 1, 2025.

(c) Secs. 5 (Vermont Data Privacy Act middle applicability threshold) and 8 (private right of action) shall take effect on July 1, 2026.

(d) Sec. 7 (cure period phase out) shall take effect on January 1, 2027.

(e) Sec. 6 (Vermont Data Privacy Act low applicability threshold) shall take effect on July 1, 2027.

(f) Sec. 9 (private right of action phase out) shall take effect on July 1, 2029.

and that after passage the title of the bill be amended to read: "An act relating to enhancing consumer privacy and the age-appropriate design code."

(Committee vote: _____)

_____

Representative _____

FOR THE COMMITTEE