TO THE HOUSE OF REPRESENTATIVES:

The Committee on Commerce and Economic Development to which was referred Senate Bill No. 71 entitled "An act relating to consumer data privacy and online surveillance" 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. DATA PRIVACY

Subchapter 1. Vermont Data Privacy and Online Surveillance Act

§ 2415a. SHORT TITLE AND DEFINITIONS

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

(b) 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) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under subdivisions 2415d(a)(1)–(5) of this subchapter 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.

(3)(A) "Biometric data" means data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that allow or confirm the unique identification of the consumer, including:

(i) iris or retina scans;

(ii) fingerprints;

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

(iv) vein patterns;

(v) voice prints or vocal biomarkers; 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.

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

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

(6)(A) "Collect" means buying, renting, gathering, obtaining, receiving, or accessing any personal data by any means, other than such activities between a controller and a processor or between a processor and its subcontractors.

(B) "Collect" includes receiving data from the consumer, either actively or passively, or by observing the consumer's behavior.

(7)(A) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, including by a statement or by a clear affirmative action, signifies agreement to the collection or processing of personal data relating to the consumer for a narrowly defined particular purpose.

(B) "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.

(8)(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 organization, 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 organization, or government agency.

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

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

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

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

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

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

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

(16) "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."

(17) "Decisions that produce legal or similarly significant effects concerning the consumer" means any decision made by the controller, or on behalf of the controller, that results in the provision or denial by the controller of any financial or lending service, any housing, any insurance, any education enrollment or opportunity, any criminal justice, any employment opportunity, or any health care services.

(18) "Deidentified 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 reidentify 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; and

(ii) for purposes of this subdivision (A), "reasonable measures" includes the deidentification 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 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.

(19) "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 consumer's device.

(20) "Financial institution" as used in subdivision 2415c(a)(13) of this title has the same meaning as in 15 U.S.C. § 6809.

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

(22) "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.

(23) "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.

(24) "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.

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

(26) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as may be amended.

(27) "Hybrid entity" has the same meaning as in HIPAA.

(28) "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, precise geolocation data, or an online identifier.

(29) "Institution of higher education" means any individual who, or school, board, association, limited liability company, or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees.

(30) "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.

(31) "Minor" means any consumer who is younger than 18 years of age.

(32) "Neural data" means any information that is generated by measuring the activity of an individual's central nervous system.

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

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

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

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

(37)(A) "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.

(B) "Personal data" does not include deidentified data or publicly available information.

(38)(A) "Precise geolocation data" means information derived from technology that reveals the past or present physical location of a consumer or device that identifies or is linked or reasonably linkable to one or more consumers with precision and accuracy 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;

(iii) a photograph, or metadata associated with a photograph or video, that cannot be linked to an individual; or

(iv) 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 use, storage, disclosure, analysis, deletion, modification, or otherwise handling of personal data.

(40) "Processor" means a person who collects or processes personal data on behalf of:

(A) a controller; or

(B) another processor.

(41) "Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects, including an

individual's economic situation, health, personal preferences, interests, reliability, behavior, location, movements, or identifying characteristics.

(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 are not attributed to an identified or identifiable individual.

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

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

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

(B) "Publicly available information" does not include:

(i) biometric data collected by a business about a consumer without the consumer's knowledge;

(ii) information that is collated and combined to create a consumer profile that is made available to a user of a publicly available website either in exchange for payment or free of charge;

(iii) information that is made available for sale;

(iv) an inference that is generated from the information described in subdivision (ii) or (iii) of this subdivision (44)(B);

(v) any obscene visual depiction, as defined in 18 U.S.C. § 1460;

(vi) personal data that is created through the combination of personal data with publicly available information;

(vii) genetic data, unless otherwise made publicly available by the consumer to whom the information pertains;

(viii) information provided by a consumer on a website or online service made available to all members of the public, for free or for a fee, where the consumer has maintained a reasonable expectation of privacy in the information, such as by restricting the information to a specific audience; or

(ix) intimate images, authentic or computer-generated, known to be nonconsensual.

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

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

(47) "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.

(48)(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.

(B) "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, with the consumer's consent, 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; or

(v) 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.

(C) As used in subdivision (B) of this subdivision (48), "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.

(49) "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, mental or physical health condition, diagnosis, disability or treatment, status as pregnant, income level or indebtedness, or union membership;

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

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

(E) is 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 collected and analyzed concerning consumer health 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 used by the controller for a purpose other than to identify a specific consumer's physical or mental health condition or diagnosis;

(H) is biometric or genetic data or information derived therefrom;

(I) is collected from a consumer who a controller knew or should have known is a minor;

(J) is precise geolocation data;

(K) is driving behavior; or

(L) is neural data.

(50)(A) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated websites or online applications to predict the consumer's preferences or interests.

(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.

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

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

(53) "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.

§ 2415b. APPLICABILITY

(a) Thresholds. Except as provided in subsection (b) of this section, this subchapter 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 35,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction;

(2) controlled or processed consumers' sensitive data, excluding personal data controlled or processed solely for the purposes of completing a payment transaction; or

(3) sold the personal data of consumers.

(b) Health data applicability. Section 2415k of this subchapter and the provisions of this subchapter 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.

(c) Controlling law. In the event of a conflict between the provisions of this subchapter and any other law, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

§ 2415c. EXEMPTIONS

(a) This subchapter does not apply to:

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

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

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

(C) a business associate;

(3) patient-identifying information, for purposes of 42 U.S.C. § 290DD–2;

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

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

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

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

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

(6) 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) 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

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

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

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

(9) 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;

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

(11) 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);

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

(C) data that is subject to 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 subchapter;

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

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

(13) 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;

(14) a state- or federally chartered bank or credit union, or an affiliate or subsidiary that is principally 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 who, alone or in combination with another person,

establishes and maintains a self-insurance program and who 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;

(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) a press association or wire service; or

(21) data processed or maintained:

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

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

(C) that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information pursuant to subdivision (2) of this subsection (a) and used for the purposes of administering such benefits.

(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 subchapter.

§ 2415d. CONSUMER PERSONAL DATA RIGHTS

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

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

(2) 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;

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

(4) 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, where the processing is carried out by automated means, provided the controller shall not be required to reveal any trade secret;

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

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

(A) targeted advertising;

(B) the sale of personal data; and

(C) profiling in furtherance of any automated decisions that produce legal or similarly significant effects concerning the consumer; and

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

(A) question the result of such profiling;

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

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

(D) if the profiling decision concerned housing, taking into account the nature of the personal data and the purposes for which such personal data

were processed, allow the consumer to correct any incorrect personal data that were processed for the purposes of such profiling and have the profiling decision reevaluated based on the corrected personal data.

(b) Exercising consumer rights.

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

(2)(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 pursuant to subsection (a) 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 right pursuant to subdivision (A) of this subdivision (2).

(C) A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

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

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

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

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

(1) Timeline to respond. A controller:

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

(B) 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) Declining to take action. 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) Cost of information.

(A) Information provided by a controller in response to a consumer request shall be provided by the 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) A controller bears the burden of demonstrating the manifestly unfounded, excessive, or repetitive nature of the request.

(4) Authentication of request.

(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) Third-party data. 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 consumer's data pursuant to subdivision (a)(3) of this section by 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 subchapter.

(6) Misrepresentation. A controller shall 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) Appeals.

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

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

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

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

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

(1) Social Security number;

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

(3) financial account number;

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

(5) account password;

(6) security question or answer thereto; or

(7) biometric data.

§ 2415e. DUTIES OF CONTROLLERS

(a) Data collection and processing.

(1) A controller:

(A) shall limit the collection and processing of a consumer's personal data:

(i) to what is reasonably necessary and proportionate to achieve the purposes for which the personal data was collected or processed, as disclosed to the consumer, which shall be consistent with the reasonable expectations of the consumer pursuant to subdivision (2) of this subsection (a); or

(ii) for another disclosed purpose that is compatible with the context in which the consumer's personal data was collected pursuant to subdivision (i) of this subdivision (A) and not further processed in a manner that is incompatible with those purposes;

(B) shall obtain the consumer's consent in accordance with this subchapter before processing the consumer's personal data for any purpose

that does not meet the requirements set forth in subdivision (A) of this subdivision (1), provided that a consumer may withdraw consent at any time and further provided that the methods for obtaining consent under this subdivision (B) shall be easy to understand, offer symmetry in choice, not use language or interactive elements that are confusing to the consumer, not use choice architecture that impairs or interferes with the consumer's ability to make a choice, and be easy to execute;

(C) may process or transfer the personal data of a consumer collected pursuant to subdivision (A) of this subdivision (1) to provide targeted advertising to the consumer, unless:

(i) the personal data is sensitive data; or

(ii) the consumer has opted out of targeted advertising pursuant to subdivision 2415d(a)(6) of this subchapter;

(D) shall 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, including disposing of personal data in accordance with a retention schedule that requires the deletion of personal data when the data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected or processed, provided that with respect to any processing of sensitive data, such reasonable

data security practices shall include, at a minimum, compliance with the most recent Privacy & Cybersecurity Frameworks for the components of the controller's information systems that process, store, or transmit sensitive data or that provide protection for such components;

(E) shall not collect or process sensitive data concerning a consumer except when the processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the sensitive data pertains;

(F) not process personal data in violation of any:

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

(ii) federal law that prohibits unlawful discrimination against consumers;

(G) shall provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent and, upon

revocation of the consent, cease to process the data as soon as practicable, but not later than 15 days after the receipt of the request;

(H) if the controller knew or willfully disregards that the consumer is a minor:

(i) shall not process the personal data of the minor for the purposes of targeted advertising; or

(ii) sell the minor's personal data, unless:

(I) the controller is a covered business and the minor is a covered minor as both terms are defined in section 2449a of this title; and

(II) the controller complies with section 2449f(a) of this title;

(I) shall not sell sensitive data;

(J)(i) except as provided in subdivision (ii) of this subdivision (J), shall not 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; and

(ii) subdivision (i) of this subdivision (J) 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 place of public accommodation);

(II) processing for the purpose of a controller's or processor's self-testing to prevent or mitigate unlawful discrimination or otherwise to ensure compliance with State or federal law; or

(III) processing for the purpose of diversifying an applicant, participant, or consumer pool; and

(K) shall not discriminate against a consumer for exercising any of the consumer rights contained in this subchapter, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

(2) As used in this subsection:

(A) "Reasonable expectations of the consumer" shall be based on the following:

(i) the relationship between the consumer and the controller;

(ii) the type, nature, and amount of the consumer's personal data that the controller seeks to collect;

(iii) the source of the consumer's personal data and the controller's method for collecting it;

(iv) the specificity, explicitness, prominence, and clarity of information provided to the consumer about the purpose for collecting the consumer's personal data; and

(v) the degree to which the involvement of processors and third parties in the collecting or processing of the consumer's personal data is apparent to the consumer.

(B) "Privacy & Cybersecurity Frameworks" means the National Institute of Standards and Technology Privacy Framework, Version 1.0, published January 2020, as well as the Cybersecurity Framework, Version 2.0, published February 2024, or any successor versions thereof.

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

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

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

(c) Privacy notice.

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

(A) the categories of personal data collected and processed by the controller, including a separate list of categories of sensitive data collected and processed by the controller, described in a level of detail that provides

consumers a meaningful understanding of the type of personal data collected and processed;

(B) the purpose for processing personal data;

(C) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;

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

(E) the categories of third parties, if any, with which the controller shares personal data; and

(F) an active email address or other online mechanism that the consumer may use to contact the controller.

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

(H) the most recent month and year during which the controller updated the privacy notice.

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

(A) through a conspicuous hyperlink that includes the word "privacy":

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

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

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

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

(C) in each language in which the controller:

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

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

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

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

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

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

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

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

(d) Targeted advertising. If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose the selling or processing, as well as the manner in which a consumer may exercise the right to opt out of the selling or processing.

(e) Providing consumers access to exercise rights.

(1) A controller shall:

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

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

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

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

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

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

(i) be consumer-friendly and easy to use by the average consumer;

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

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

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

(4) If a controller responds to a consumer opt-out request received pursuant to subdivision (2)(C) of this subsection by informing the consumer of a charge for the use of any product or service, the controller shall present the

terms of any financial incentive offered pursuant to subdivision (b)(2) of this section for the retention, use, sale, or sharing of the consumer's personal data.

§ 2415f. PROCESSORS' DUTIES; CONTRACTS BETWEEN CONTROLLERS AND PROCESSORS

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

(1) taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, to the extent reasonably practicable, to fulfill the controller's obligation to respond to consumer rights requests;

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

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

(b) Contractual terms.

(1) A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The processor shall adhere to the instructions of the controller and only process and transfer the data it receives from the controller to the extent necessary to provide a service requested by the controller, as set out in the contract.

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

(3) The contract shall require that the processor:

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

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

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

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

(E) unless consent is given by the consumer, be prohibited from combining personal data obtained from the controller with personal data that the processor:

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

(ii) collects directly from the consumer; and

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

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

(c) Liabilities. This section shall not 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 this subchapter.

(d) Processors performing as controllers.

(1) 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.

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

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

(4) 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 2415j of this subchapter.

§ 2415g. DATA PROTECTION AND IMPACT ASSESSMENTS; DISCLOSURE TO ATTORNEY GENERAL

(a) Generally. 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) Requirements.

(1) Data protection assessments conducted pursuant to subsection (a) of this section shall 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 rights of 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 deidentified 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) Impact assessments for profiling. Each controller that engages in any profiling for the purposes of making a decision that produces any legal or

similarly significant effect concerning a consumer shall conduct an impact assessment for the profiling. The impact assessment shall include, to the extent reasonably known by or available to the controller, as applicable:

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

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

(A) the nature of such heightened risk of harm to a consumer; and

(B) the steps that have been taken to mitigate such heightened risk of harm to a consumer;

(3) a description of:

(A) the main categories of personal data processed as inputs for the purposes of such profiling; and

(B) the outputs such profiling produces;

(4) an overview of the main categories of personal data the controller used to customize the profiling, if the controller used data to customize the profiling;

(5) any metrics used to evaluate the performance and known limitations of the profiling;

(6) a description of any transparency measures taken concerning the profiling, including any measures taken to disclose to consumers that the

controller is engaged in profiling while the controller is engaged in the profiling; and

(7) a description of the post deployment monitoring and user safeguards provided concerning such profiling, including, but not limited to, the oversight, use, and learning processes established by the controller to address issues arising from such profiling.

(d) Disclosure to Attorney General.

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

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

(3) Data protection and impact 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 or impact 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) Assessment efficiency and applicability.

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

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

(3) Data protection and impact assessment requirements shall apply to processing activities created or generated after July 1, 2026, and are not retroactive.

(f) Updating assessment. A controller shall update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of personal data collected or processed and level of risk presented by the processing throughout the processing activity's lifecycle in order to:

(1) monitor for harm caused by the processing and adjust safeguards accordingly; and

(2) ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing.

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

(h) Independent validation for processing sensitive data.

(1) In addition to the requirements of this section, for any data protection assessment that addresses the processing of sensitive data, the controller shall ensure that the assessment includes an evaluation and validation of the controller's compliance with the minimum cybersecurity baseline set forth in subdivision 2415e(a)(1)(D) of this subchapter, as it applies to sensitive data.

(2) For an assessment described in subdivision (1) of this subsection, the evaluation of compliance shall be conducted or reviewed and validated by a qualified and independent person. The qualified and independent person shall provide a written validation report to the controller that, at a minimum:

(A) identifies the information system components assessed and the scope of sensitive data processing covered;

(B) states whether the qualified and independent person finds compliance with the minimum cybersecurity baseline set forth in subdivision 2415e(a)(1)(D) of this subchapter, as it applies to sensitive data, and, if not, identifies material gaps; and

(C) identifies remediation measures and a reasonable schedule for remediation of any material gaps.

(3) The validation report pursuant to subdivision (2) of this subsection and any supporting documentation shall be deemed part of the data protection

assessment for purposes of confidentiality, privilege, and retention under this section.

(4) A controller that knowingly fails to comply with this subsection by either not completing a validation when so required or including false information in a data protection assessment commits fraud and is subject to the penalties pursuant to subsection 2415j(b) of this subchapter.

§ 2415h. DEIDENTIFIED DATA

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

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

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

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

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

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

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

(3) require a controller or processor to 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; and

(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.

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

§ 2415i. CONSTRUCTION OF DUTIES

(a) Generally. This subchapter 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, except as prohibited by 1 V.S.A. § 150;

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

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

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

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

(8) 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;

(9) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious, or deceptive activities or any illegal 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;

(10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws

and is approved, monitored, and governed by an institutional review board that determines, or similar independent oversight entities that determine:

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

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

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

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

(12) 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; or

(13) collect, use, or retain data for internal use to:

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

(B) effectuate a product recall;

(C) identify and repair technical errors that impair existing or intended functionality;

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

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

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

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

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

(v) not transmitted, transferred, or otherwise accessed by any third party;

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

(F) perform internal operations in accordance with the internal operations exception established in COPPA if the controller, processor, or consumer health data controller is processing data in accordance with the exception.

(b) Evidentiary privilege.

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

(2) This subchapter 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 subchapter modifies 2020 Acts and Resolves No. 166, Sec. 14 or authorizes the use of facial recognition technology by law enforcement.

(c) Third parties.

(1) A controller, processor, or consumer health data controller that discloses personal data to a processor or third-party controller pursuant to this subchapter shall not be deemed to have violated this subchapter if the processor or third-party controller that receives and processes the personal data violates this subchapter, 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 subchapter.

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

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

(1) impose any obligation on a controller or processor 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;

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

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

(e) Personal data processing.

(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) reasonably necessary and proportionate 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 subdivision (a)(13) of this section shall, where applicable, take into account the nature and purpose or purposes of the collection, use, or retention.

(B) The data 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.

(3) 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 of this subsection.

(4) 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.

§ 2415j. ENFORCEMENT

(a) Consumer Protection Act.

(1) A violation of the requirements of this subchapter shall constitute an unfair and deceptive act in commerce in violation of section 2453 of this title and shall be enforced solely by the Attorney General, subject to the exception set forth in subdivision (2) of this subsection.

(2) Pursuant to subsection 2461(b) of this title, a consumer may bring a civil claim for a violation of the requirements of this subchapter only against a person whose annual gross revenues exceeded $1,000,000,000.00 in the previous calendar year.

(3) The Attorney General has the same authority to adopt rules to implement the provisions of this subchapter 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.

(b) Penalty for fraud. A controller that has knowingly committed fraud pursuant to subdivision 2415g(h)(4) of this subchapter shall be liable to the State for:

(1) a civil penalty of not less than $10,000.00 and not more than $25,000.00 for each act constituting a violation;

(2) three times the amount of damages that the State sustains because of the act of the controller; and

(3) the costs of the investigation and prosecution of such violation.

(c) Reporting. 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 pursuant to this subchapter that the Attorney General has issued;

(2) the nature of each violation;

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

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

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

§ 2415k. CONSUMER HEALTH DATA PRIVACY

Except as provided in section 2415i of this subchapter and subsection 2415c(b) of this subchapter, 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 2415f of this subchapter; 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. EFFECTIVE DATE

This act shall take effect on January 1, 2028.

(Committee vote: _____)

_____

Representative _____

FOR THE COMMITTEE