S.269

Introduced by Senators Clarkson, Harrison, Perchlik, Ram Hinsdale, Watson and Wrenner

Referred to Committee on

Date:

Subject: Commerce and trade; consumer protection

Statement of purpose of bill as introduced: This bill proposes to afford data privacy protections to Vermonters.

An act relating to enhancing consumer privacy

It is hereby enacted by the General Assembly of the State of Vermont:

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) "Authenticate" means to use reasonable means to determine that a request to exercise any of the rights afforded under subdivisions 2418(a)(1) through (4) 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.

(3)(A) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that are used to identify a specific individual.

(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 the data is generated to identify a specific individual.

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

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

(6)(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.

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

(8) "Controller" means an individual who, or legal entity that, alone or jointly with others, determines the purpose and means of processing personal data.

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

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

(11) "Dark pattern":

(A) means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice; and

(B) includes any practice the Federal Trade Commission refers to as a "dark pattern."

(12) "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.

(13) "De-identified data" means data that 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) takes reasonable measures to ensure that the data cannot be associated with an individual;

(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 (13).

(14) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d et seq., as amended from time to time.

(15) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

(16) "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.

(17) "Nonprofit organization" means any organization that is exempt from taxation under Section 501(c)(3), 501(c)(4), 501(c)(6), or 501(c)(12) of

the Internal Revenue Code of 1986, or any subsequent corresponding internal revenue code of the United States, as amended from time to time.

(18)(A) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual.

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

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

(B) "Precise geolocation data" does not include the content of communications or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(20) "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.

(21) "Processor" means an individual who, or legal entity that, processes personal data on behalf of a controller.

(22) "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.

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

(24) "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.

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

(A) is lawfully made available through federal, state, or municipal government records or widely distributed media; and

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

(26)(A) "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a third party.

(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 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.

(27) “Sensitive data” means personal data that includes:

(A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status;

(B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual;

(C) personal data collected from a known child; or

(D) precise geolocation data.

(28)(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) advertisements based on activities within a controller's own websites or online applications;

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

(iii) advertisements 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.

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

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

§ 2416. APPLICABILITY

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 less than 100,000 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 less than 25,000 consumers and derived more than 25 percent of the person's gross revenue from the sale of personal data.

§ 2417. EXEMPTIONS

(a) This chapter shall not apply to:

(1) a national securities association that is registered under 15 U.S.C. § 78o-3 of the Securities Exchange Act of 1934, as amended from time to time;

(2) a financial institution or data subject to Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq.; or

(3) a covered entity or business associate, as defined in 45 C.F.R. § 160.103.

(b) The following information and data are exempt from the provisions of this chapter:

(1) protected health information under HIPAA;

(2) patient-identifying information for purposes of 42 U.S.C. § 290dd-2;

(3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. § 46;

(4) identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use;

(5) the protection of human subjects under 21 C.F.R. Parts 50 and 56, or personal data used or shared in research, as defined in 45 C.F.R. § 164.501, that is conducted in accordance with the standards set forth in this subdivision and subdivisions (3) and (4) of this subsection, or other research conducted in accordance with applicable law;

(6) information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. § 11101 et seq.;

(7) patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 U.S.C. § 299b-21 et seq., as amended from time to time;

(8) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

(9) information originating from and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this subsection that is maintained by a covered entity or business associate, program, or qualified service organization, as specified in 42 U.S.C. § 290dd-2, as amended from time to time;

(10) information used for public health activities and purposes as authorized by HIPAA, community health activities, and population health activities;

(11) the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, furnisher, or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., as amended from time to time;

(12) personal data collected, processed, sold, or disclosed in compliance with the Driver’s Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq., as amended from time to time;

(13) personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g et seq., as amended from time to time;

(14) personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act, 12 U.S.C. § 2001 et seq., as amended from time to time;

(15) data processed or maintained:

(A) in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, 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 an individual under this chapter, 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 under subdivision (1) of this subsection (b) and used for the purposes of administering the benefits; and

(16) personal data collected, processed, sold, or disclosed in relation to price, route, or service, as the terms are used in the Airline Deregulation Act, 49 U.S.C. § 40101 et seq., as amended from time to time, by an air carrier subject to the act, to the extent a provision of this chapter is preempted by the Airline Deregulation Act, 49 U.S.C. § 41713, as amended from time to time.

(c) Controllers and processors 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.

§ 2418. CONSUMER’S RIGHTS; COMPLIANCE BY CONTROLLERS; APPEALS

(a) A consumer may:

(1) confirm whether or not a controller is processing the consumer’s personal data and access the personal data, unless the confirmation or access would require the controller to reveal a trade secret;

(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;

(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; and

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

(A) targeted advertising;

(B) the sale of personal data, except as provided in subsection 2420(b) of this title; 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 a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice.

(2) A consumer may designate an authorized agent in accordance with section 2419 of this title to exercise the rights of the consumer to opt out of the processing of the consumer's personal data for purposes of subdivision (a)(5) of this section on behalf of the consumer.

(3) In the case of processing personal data of a known child, the parent or legal guardian may exercise the consumer rights on the child's behalf.

(4) In the case of processing personal data concerning a consumer 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) 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)–(4) 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)(3) 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.

(d)(1) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request 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 appeal is denied, 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.

§ 2419. AUTHORIZED AGENTS AND CONSUMER OPT-OUT

(a) A consumer may designate another person to serve as the consumer's authorized agent, and act on the consumer's behalf, to opt out of the processing of the consumer’s personal data for one or more of the purposes specified in subdivision 2418(a)(5) of this title.

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

(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.

§ 2420. CONTROLLERS’ DUTIES; SALE OF PERSONAL DATA TO THIRD PARTIES; NOTICE AND DISCLOSURE TO CONSUMERS; CONSUMER OPT-OUT

(a) A controller:

(1) shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer;

(2) except as otherwise provided in this chapter, shall not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is

processed, as disclosed to the consumer, unless the controller obtains the consumer’s consent;

(3) 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;

(4) shall not process sensitive data concerning a consumer without obtaining the consumer’s consent or, in the case of the processing of sensitive data concerning a known child, without processing the data in accordance with COPPA;

(5) shall not process personal data in violation of the laws of this State and federal laws that prohibit unlawful discrimination against consumers;

(6) 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;

(7) shall not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer’s personal data without the consumer’s consent, under circumstances where a controller has actual

knowledge, and willfully disregards, that the consumer is at least 13 years of age but younger than 16 years of age; and

(8) shall not discriminate against a consumer for exercising any of the consumer rights contained in this chapter, 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.

(b) Subsection (a) of this section shall not be construed to 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 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) A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

(1) the categories of personal data processed by the controller;

(2) the purpose for processing personal data;

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

(4) the categories of personal data that the controller shares with third parties, if any;

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

(6) an active e-mail address or other online mechanism that the consumer may use to contact the controller.

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

(e)(1) A controller shall 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 chapter.

(2) The means shall 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.

(3) A controller shall 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.

(4)(A) The means shall include:

(i) providing a clear and conspicuous link on the controller’s website to an web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer’s personal data; and

(ii) not later than January 1, 2026, allowing 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 the processing or sale, by a platform, technology, or other mechanism that shall:

(I) not unfairly disadvantage another controller;

(II) not make use of a default setting, but rather require the consumer to make an affirmative, freely given, and unambiguous choice to opt out of any processing of the consumer’s personal data pursuant to this chapter;

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

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

(V) 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.

(B) 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 (A) of this subdivision (e)(4) 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.

(5) If a controller responds to consumer opt-out requests received pursuant to subdivision (4)(A) 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 subsection (b) of this section for the retention, use, sale, or sharing of the consumer’s personal data.

§ 2421. PROCESSORS' DUTIES; CONTRACTS BETWEEN CONTROLLERS AND PROCESSORS

(a) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter, 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 assessments.

(b)(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.

(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 chapter;

(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; and

(E) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for the assessments.

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

(c) 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 chapter.

(d)(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 2425 of this title.

§ 2422. CONTROLLERS' DATA PROTECTION ASSESSMENTS; DISCLOSURE TO ATTORNEY GENERAL

(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 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 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, 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 include similar activities.

(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, 2024 and are not retroactive.

§ 2423. DE-IDENTIFIED AND PSEUDONYMOUS DATA; CONTROLLERS' DUTIES; EXCEPTIONS; APPLICABILITY OF CONSUMERS' RIGHTS; DISCLOSURE AND OVERSIGHT

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

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

(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 chapter shall not be construed to:

(1) require a controller or processor to re-identify de-identified data or pseudonymous data; or

(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.

(c) This chapter shall not be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

(1) 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;

(2) 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

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

(d) The rights afforded under subdivisions 2418(a)(1) to (4) 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 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.

§ 2424. CONSTRUCTION OF CONTROLLERS' AND PROCESSORS' DUTIES

(a) This chapter shall not be construed to restrict a controller's or processor'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 or processor 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; 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 has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

(11) assist another controller, processor, or third party with any of the obligations under this chapter; or

(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.

(b) The obligations imposed on controllers or processors under this chapter shall not restrict a controller's or processor'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;

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

(4) 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 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.

(c)(1) The obligations imposed on controllers or processors under this chapter shall not apply where compliance by the controller or processor 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 or processor 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.

(d)(1) A controller or processor 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 or processor disclosed the personal data, the disclosing controller or processor 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 or processor in compliance with this chapter is not in violation of this chapter for the transgressions of the controller or processor 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 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 United States 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 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 subsection (b) 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.

(g) If a controller processes personal data pursuant to an exemption in this section, the 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 with respect to the processing.

§ 2425. ENFORCEMENT BY ATTORNEY GENERAL; NOTICE OF VIOLATION; CURE PERIOD; REPORT; PENALTY

(a) The Attorney General shall have exclusive authority to enforce violations of this chapter.

(b)(1) During the period beginning on July 1, 2024 and ending on December 31, 2025, the Attorney General shall, prior to initiating any action for a violation of any provision of this chapter, issue a notice of violation to the controller if the Attorney General determines that a cure is possible.

(2) If the controller fails to cure the violation within 60 days after receipt of the notice of violation, the Attorney General may bring an action pursuant to this section.

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

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

(B) the nature of each violation;

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

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

(c) Beginning on January 1, 2026, the Attorney General may, in determining whether to grant a controller or processor the opportunity to cure an alleged violation described in subsection (b) of this section, consider:

(1) the number of violations;

(2) the size and complexity of the controller or processor;

(3) the nature and extent of the controller's or processor's processing activities;

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

(5) the safety of persons or property; and

(6) whether the alleged violation was likely caused by human or technical error.

(d) This chapter shall not be construed as providing the basis for, or be subject to, a private right of action for violations of this chapter or any other law.

(e) A violation of the requirements of this chapter 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, provided that a consumer private right of action under subsection 2461(b) of this title shall not apply to the violation.

Sec. 2. 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 identifier” means unique biometric data generated from measurements or technical analysis of an individual’s biological characteristics, including a fingerprint, voiceprint, retina, iris, or other unique biological characteristics, which is used to identify a specific individual.

(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, the as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data~~ biometric identifier;

(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 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.

~~(4)~~(5)(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)~~(6)(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, the as fraudulent accounts opened or instances of identity theft reported; or

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

~~(6)~~(7) "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)~~(8) “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)~~(9) “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)~~(10) “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)~~(11)(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, the as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data~~ a biometric identifier;

(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.

~~(11)~~(12) “Record” means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

~~(12)~~(13) “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)~~(14)(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, the 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, the 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 (d) 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 subdivision (3) and subdivision (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 one 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; or

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

(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. The Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations made 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.

* * *

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~~ the method for 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, and sales activities~~, and opt-out policies~~ that are applicable to the brokered personal information of minors; and

~~(G)~~(D) 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~~ $100.00 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 five 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 five 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; ADDITIONAL DUTIES

(a) Individual opt-out.

(1) A consumer may request that a data broker do any of the following:

(A) stop collecting the consumer's data;

(B) delete all data in its possession about the consumer; or

(C) stop selling the consumer’s data.

(2) A data broker shall establish a simple procedure for consumers to submit a request and shall comply with a request from a consumer within 10 days after receiving the request.

(3) A data broker shall clearly and conspicuously describe the opt-out procedure in its annual registration and on its website.

(b) General opt-out.

(1) A consumer may request that all data brokers registered with the State of Vermont honor an opt-out request by filing the request with the Secretary of State.

(2) The Secretary of State shall develop an online form to facilitate the general opt-out by a consumer and shall maintain a data broker opt-out list of consumers who have requested a general opt-out, with the specific type of opt-out included.

(3) The data broker opt-out list shall contain the minimum amount of information necessary for a data broker to identify the specific consumer making the opt-out.

(4) Once every 31 days, any data broker registered with the State of Vermont shall review the data broker opt-out list in order to comply with the opt-out requests contained therein.

(5) Data contained in the data broker opt-out list shall not be used for any purpose other than to effectuate a consumer’s opt-out request.

(c) 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 consumer report will not be used for a legitimate and legal purpose.

(d) Exemption. Nothing in this section applies to brokered personal information that is regulated as a consumer report pursuant to the Fair Credit Reporting Act, if the data broker is fully complying with the Fair Credit Reporting Act.

Subchapter 6. Biometric Information

§ 2449. PROTECTION OF BIOMETRIC INFORMATION

(a) Collection, use, and retention of biometric identifiers.

(1) A person shall not collect or retain a biometric identifier without first providing clear and conspicuous notice pursuant to this section and providing a mechanism to opt out of the subsequent use of a biometric identifier.

(2) A person providing notice pursuant to subdivision (1) of this subsection shall include:

(A) a description of the biometric identifiers being collected or retained;

(B) the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, or used;

(C) the third parties to which the biometric identifier may be sold, leased, or otherwise disclosed to and the purpose of the disclosure; and

(D) the mechanism by which the consumer may opt out of the subsequent use of the biometric identifier.

(3) A person who has collected or stored a consumer's biometric identifier may not use, sell, lease, or otherwise disclose the biometric identifier to another person if a consumer has exercised the consumer's right to opt out of the subsequent use of a biometric identifier.

(4) A person who possesses a biometric identifier of a consumer:

(A) shall take reasonable care to guard against unauthorized access to and acquisition of biometric identifiers that are in the possession or under the control of the person;

(B) shall adopt a comprehensive information security program that complies with section 2447 of this title; and

(C) may retain the biometric identifier not longer than is reasonably necessary to:

(i) comply with a court order, statute, or public records retention schedule specified under federal, state, or local law;

(ii) protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; and

(iii) provide the services for which the biometric identifier was collected or stored.

(5)(A) A person who collects or retains biometric identifiers shall establish a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining the identifiers or information has been satisfied or within one year following the consumer’s last interaction with the person, whichever occurs first.

(B) Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a person who possesses biometric identifiers or biometric information shall comply with its established retention schedule and destruction guidelines.

(6) A person who collects or stores a biometric identifier of a consumer or obtains a biometric identifier of a consumer from a third party pursuant to this section may not use or disclose it in a manner that is materially inconsistent with the terms under which the biometric identifier was originally provided without disclosing the new terms of use or disclosure and providing a mechanism to opt out of the new use of the biometric identifier.

(7) Nothing in this section requires a person to provide notice to a consumer if:

(A) the biometric identifier will be used solely to authenticate the consumer for the purpose of securing the goods or services provided by the business;

(B) the biometric identifier will not be leased or sold to any third party; and

(C) the biometric identifier will only be disclosed to a third party for the purpose of effectuating subdivision (A) of this subdivision (a)(7), and the third party is contractually obligated to maintain the confidentiality of the biometric identifier and to not further disclose the biometric identifier.

(b) Enforcement.

(1)(A) The Attorney General and State’s Attorney shall have authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations made 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 (b).

(B) In determining appropriate civil penalties, the courts shall consider each instance in which a person violates this subchapter with respect to each consumer as a separate violation and shall base civil penalties on the seriousness of the violation, the size and sophistication of the business violating the subchapter, and the business’s history of respecting or failing to respect the privacy of consumers, with maximum penalties imposed where appropriate.

(C) A person who possesses a biometric identifier of a consumer that was not acquired in accordance with the requirements of this subchapter as of the effective date of this law shall either obtain consent or delete the biometric information within 180 days after enactment of this law or shall be liable for $10,000.00 per day thereafter until the business has complied with this subdivision (b)(1)(C).

(2) A consumer aggrieved by a violation of this subchapter or rules adopted under this subchapter may bring an action in Superior Court for the consumer’s damages, injunctive relief, punitive damages, and reasonable costs and attorney’s fees. The court, in addition, may issue an award for the greater of the consumer’s actual damages or $1,000.00 for a negligent violation or $5,000.00 for a willful or reckless violation.

(c) Exclusions. Nothing in this chapter expands or limits the authority of a law enforcement officer acting within the scope of the officer’s authority, including the authority of a State law enforcement officer in executing lawful searches and seizures.

Sec. 3. EFFECTIVE DATE

This act shall take effect on July 1, 2024.