H.121

Senator Lyons moves that the Senate proposal of amendment be amended as follows:

First: In Sec. 1, 9 V.S.A. chapter 61A, by striking out section 2415 in its entirety and inserting in lieu thereof a new section 2415 to read:

§ 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)–

(5) of this title is being made by, or on behalf of, the consumer who is entitled to exercise the consumer rights with respect to the personal data at issue.

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

(A) iris or retina scans;

(B) fingerprints;

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

(D) vein patterns;

(E) voice prints;

(F) gait or personally identifying physical movement or patterns;

(G) depictions, images, descriptions, or recordings; and

(H) data derived from any data in subdivision (G) of this subdivision (3), to the extent that it would be reasonably possible to identify the specific individual from whose biometric data the data has been derived.

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

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

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

(7)(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.

(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, 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.

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

(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 promulgated 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 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.

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

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

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

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

(C) contractually obligates any recipients of the data to satisfy the criteria set forth in subdivisions (A) and (B) of this subdivision (18).

(19) "Educational institution" has the same meaning as "educational agency or institution" in 20 U.S.C. § 1232g (family educational and privacy rights);

(20) "Financial institution":

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

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

(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 component" has the same meaning as in HIPAA.

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

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

(A) material physical or financial injury to a minor;

(B) emotional distress, as that term is defined in 13 V.S.A. § 1061(2), to a minor;

(C) a highly offensive intrusion on the reasonable privacy expectations of a minor;

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

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

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

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

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

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

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

(33) "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.

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

(35)(A) "Online service, product, or feature" means any service, product, or feature that is provided online, except as provided in subdivision (B) of this subdivision (35).

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

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

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

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

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

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

(38)(A) "Personal data" means any information, including derived data and unique identifiers, that is linked or reasonably linkable to an identified or identifiable individual or to a device that identifies, is linked to, or is

reasonably linkable to one or more identified or identifiable individuals in a household.

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

(39)(A) "Precise geolocation data" means personal data derived from technology that accurately identifies within a radius of 1,850 feet a consumer's present or past location or the present or past location of a device that links or is linkable to a consumer or any data that is derived from a device that is used or intended to be used to locate a consumer within a radius of 1,850 feet by means of technology that includes a global positioning system that provides latitude and longitude coordinates.

(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.

(40) "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.

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

(42) "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.

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

(44) "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.

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

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

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

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

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

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

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

(49) "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.

(50)(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 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.

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

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

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

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

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

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

(F) is consumer health data;

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

(H) is biometric or genetic data;

(I) is personal data collected from a known child;

(J) is a photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of a consumer; or

(K) is precise geolocation data.

(52)(A) "Targeted advertising" means displaying an advertisement 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 internet 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 a controller's own websites or online applications;

(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.

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

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

(55) "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.

Second: In Sec. 1, 9 V.S.A. chapter 61A, in subsection 2417(a), by striking out subdivision (2) in its entirety and inserting in lieu thereof a new subdivision (2) to read:

(2) a covered entity that is not a hybrid entity, any health care component of a hybrid entity, or a business associate;

Third: In Sec. 1, 9 V.S.A. chapter 61A, in subsection 2417(a), by striking out subdivision (8) in its entirety and inserting in lieu thereof a new subdivision (8) to read:

(8) information that originates from, or is intermingled so as to be indistinguishable from, information described in subdivisions (3)–(7) of this subsection that a covered entity, business associate, or a qualified service organization program creates, collects, processes, uses, or maintains in the same manner as is required under the laws, regulations, and guidelines described in subdivisions (3)–(7) of this subsection;

Fourth: In Sec. 1, 9 V.S.A. chapter 61A, by striking out section 2425 in its entirety and inserting in lieu thereof a new section 2425 to read:

§ 2425. ENFORCEMENT: ATTORNEY GENERAL'S POWERS AND PRIVATE RIGHT OF ACTION

(a) A person who violates this chapter or rules adopted pursuant to this chapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title, and the Attorney General shall have exclusive authority to enforce such violations except as provided in subsection (c) of this section.

(b)(1) If the Attorney General determines that a violation of this chapter or rules adopted pursuant to this chapter may be cured, the Attorney General may, prior to initiating any action for the violation, issue a notice of violation

extending a 60-day cure period to the controller, processor, or consumer health data controller alleged to have violated this chapter or rules adopted pursuant to this chapter.

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

(A) the number of violations;

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

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

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

(E) the safety of persons or property;

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

(G) the sensitivity of the data.

(c)(1) The private right of action available to a consumer for violations of this chapter or rules adopted pursuant to this chapter shall be exclusively as provided under this subsection.

(2) A consumer who is harmed by a violation of subdivision 2419(b)(2) of this title or section 2426 of this title may bring an action under subsection 2461(b) of this title for the violation, but the right available under subsection 2461(b) of this title shall not be available for a violation of any other provision of this chapter or rules adopted pursuant to this chapter.

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

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

(2) the nature of each violation;

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

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

Fifth: In Sec. 1, 9 V.S.A. chapter 61A, in subdivision 2426(3), following "any health care facility," by striking out "mental health facility, or reproductive or sexual health facility" and inserting in lieu thereof including any mental health facility or reproductive or sexual health facility,

Sixth: In Sec. 2, 3 V.S.A. § 5023, by striking out subsections (a) and (b) in their entireties and inserting in lieu thereof new subsections (a) and (b) to read:

(a)(1) Advisory Council. There is established the Artificial Intelligence and Data Privacy Advisory Council to:

(A) provide advice and counsel to the Director of the Division of Artificial Intelligence ~~with regard to~~ on the Division's responsibilities to review all aspects of artificial intelligence systems developed, employed, or procured in State government~~.~~;

(B) ~~The Council,~~ in consultation with the Director of the Division, ~~shall also~~ engage in public outreach and education on artificial intelligence;

(C) provide advice and counsel to the Attorney General in carrying out the Attorney General's enforcement responsibilities under the Vermont Data Privacy Act; and

(D) engage in research on data privacy and develop policy recommendations for improving data privacy in Vermont, including:

(i) development of education and outreach to consumers and businesses on the Vermont Data Privacy Act; and

(ii) recommendations for improving the scope of health-care exemptions under the Vermont Data Privacy Act, including based on:

(I) research on the effects on the health care industry of the health-related data-level exemptions under the Oregon Consumer Privacy Act;

(II) economic analysis of compliance costs for the health care industry; and

(III) an analysis of health-related entities excluded from the health-care exemptions under 9 V.S.A. § 2417(a)(2)–(8).

(2)(A) The Advisory Council shall report its findings and any recommendations under subdivision (1)(D) of this subsection (a) to the Senate Committees on Economic Development, Housing and General Affairs, on Health and Welfare, and on Judiciary and the House Committees on Commerce and Economic Development, on Health Care, and on Judiciary on or before January 15, 2025.

(B) The Advisory Council shall have the authority to establish subcommittees to carry out the purposes of subdivision (1)(D) of this subsection (a).

(b) Members.

(1) Members. The Advisory Council shall be composed of the following members:

(A) the Secretary of Digital Services or designee;

(B) the Secretary of Commerce and Community Development or designee;

(C) the Commissioner of Public Safety or designee;

(D) the Executive Director of the American Civil Liberties Union of Vermont or designee;

(E) one member who is an expert in constitutional and legal rights, appointed by the Chief Justice of the Supreme Court;

(F) one member with experience in the field of ethics and human rights, appointed by the Governor;

(G) one member who is an academic at a postsecondary institute, appointed by the Vermont Academy of Science and Engineering;

(H) the Commissioner of Health or designee;

(I) the Executive Director of Racial Equity or designee; ~~and~~

(J) the Attorney General or designee;

(K) the Secretary of Human Services or designee;

(L) one member representing Vermont small businesses, appointed by the Speaker of the House; and

(M) one member who is an expert in data privacy, appointed by the Committee on Committees.

(2) Chair. Members of the Advisory Council shall elect by majority vote the Chair of the Advisory Council. Members of the Advisory Council shall be appointed on or before August 1, 2022 in order to prepare as they deem necessary for the establishment of the Advisory Council, including the election of the Chair of the Advisory Council, except that the members appointed under subdivisions (K)–(M) of subdivision (1) of this subsection shall be appointed on or before August 1, 2024.

(3) Qualifications. Members shall be drawn from diverse backgrounds and, to the extent possible, have experience with artificial intelligence.