TO THE HOUSE OF REPRESENTATIVES:

The Committee on Commerce and Economic Development to which was referred Senate Bill No. 110 entitled "An act relating to data privacy" respectfully reports that it has considered the same and recommends that the House propose to the Senate that the bill be amended by striking out all after the enacting clause and inserting in lieu thereof the following:

* * * Data Privacy; State Government * * *

Sec. 1. DATA PRIVACY INVENTORY

(a) On or before January 15, 2020, the following persons shall e conduct a data privacy inventory and submit a report for their respective branches of State government to the House Committees on Commerce and Economic Development and on Government Operations and to the Senate Committees on Economic Development, Housing and General Affairs and on Government Operations:

(1) the State Court Administrator for the judicial branch;

(2) the Deputy Director for Information Technology within the Office of Legislative Council for the legislative branch; and

(3) the Chief Data Officer within the Agency of Digital Services and the Chief Records Officer within the Office of the Secretary of State for the executive branch.

(b) The inventory and report for each branch shall address the collection and management of personally identifiable information, as defined in 9 V.S.A. § 2430(9), and of street addresses, e-mail addresses, telephone numbers, and demographic information, specifically:

(1) federal and State laws, rules, and regulations that:

(A) exempt personally identifiable information from public inspection and copying pursuant to 1 V.S.A. § 317;

(B) require personally identifiable information to be produced or acquired in the course of State government business;

(C) specify fees for obtaining personally identifiable information produced or acquired in the course of State government business; and

(D) require personally identifiable information to be shared between branches of State government or between branches and non-state entities, including municipalities;

(2) arrangements or agreements, whether verbal or written, between branches of State government or between branches and non-state entities, including municipalities, to share personally identifiable information, street addresses, e-mail addresses, telephone numbers, and demographic information; and

(3) recommendations for proposed legislation concerning the collection and management of personally identifiable information, street addresses, e-

mail addresses, telephone numbers, and demographic information ~~by all three branches of State government~~.

~~* * * Security Breach Notice Act * * *~~

Sec. 2. 9 V.S.A. § 2430(9) is amended to read:

(9)(A) "Personally identifiable information" means a consumer's first name or first initial and last name, or a consumer's Social Security number, in combination with ~~any~~ one or more of the following digital data elements, ~~when either the name~~ if the Social Security number or the data elements are not encrypted, ~~or~~ redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons:

(i) ~~Social Security number~~ a driver license or identification number, passport number, military identification number, or other similar [government-issued] number [issued on a government document and] used to verify identity;

(ii) ~~motor vehicle operator's license number or nondriver identification card number~~ a health insurance policy number;

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

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

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

(vi) genetic information;

(vii) ~~health~~ information about a consumer's medical history, mental condition, or physical condition, or about a health care professional's medical diagnosis or treatment of the consumer; and

(viii) ~~login credentials, including a username or password; and~~ a user name or email address, in combination with a password or an answer to a security question, that together permit access to an online account.

~~(ix) a passport 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.

Sec. 3. 9 V.S.A. § 2435 is amended to read:

§ 2435. NOTICE OF SECURITY BREACHES

(a) This section shall be known as the Security Breach Notice Act.

(b) Notice of breach.

(1) Except as set forth in subsection (d) of this section, any data collector that owns or licenses computerized personally identifiable information that includes personal information concerning a consumer shall notify the consumer that there has been a security breach following discovery or notification to the data collector 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 (b), 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) Any data collector that maintains or possesses computerized data containing personally identifiable information of a consumer that the data collector does not own or license or any data collector that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable information that the data collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subdivisions (3) and (4) of this subsection (b).

(3) A data collector or other entity subject to this subchapter shall provide notice of a breach to the Attorney General or to the Department of Financial Regulation, as applicable, as follows:

(A) A data collector or other entity regulated by the Department of Financial Regulation under Title 8 or this title shall provide notice of a breach to the Department. All other data collectors or other entities subject to this subchapter shall provide notice of a breach to the Attorney General.

(B)(i) The data collector shall notify the Attorney General or the Department, as applicable, 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 this subdivision (3) and subdivision (4) of this subsection (b), of the data collector's discovery of the security breach or when the data collector provides notice to consumers pursuant to this section, whichever is sooner.

(ii) Notwithstanding subdivision (B)(i) of this subdivision (b)(3), a data collector who, prior to the date of the breach, on a form and in a manner prescribed by the Attorney General, had sworn in writing to the Attorney General that it maintains written policies and procedures to maintain the security of personally identifiable information and respond to a breach in a manner consistent with Vermont law shall notify the Attorney General of the

date of the security breach and the date of discovery of the breach and shall provide a description of the breach prior to providing notice of the breach to consumers pursuant to subdivision (1) of this subsection (b).

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

(iv) Unless otherwise ordered by a court of this State for good cause shown, a notice provided under this subdivision (3)(B) shall not be disclosed to any person other than the Department, 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 collector.

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

(ii) The data collector may send to the Attorney General or the Department, as applicable, a second copy of the consumer notice, from which is redacted the type of personally identifiable information that was subject to

the breach, and which the Attorney General or the Department shall use for any public disclosure of the breach.

(4)(A) 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 collector shall document such request contemporaneously in writing, including 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 collector 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 collector 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.

(B) A Vermont law enforcement agency with a reasonable belief that a security breach has or may have occurred at a specific business shall notify

the business in writing of its belief. The agency shall also notify the business that additional information on the security breach may need to be furnished to the Office of the Attorney General or the Department of Financial Regulation and shall include the website and telephone number for the Office and the Department in the notice required by this subdivision. Nothing in this subdivision shall alter the responsibilities of a data collector under this section or provide a cause of action against a law enforcement agency that fails, without bad faith, to provide the notice required by this subdivision.

(5) The notice to a consumer shall be clear and conspicuous. The notice shall include a description of each of the following, if known to the data collector:

(A) the incident in general terms;

(B) the type of personally identifiable information that was subject to the security breach;

(C) the general acts of the data collector to protect the personally identifiable 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 security breach.

(6) A data collector may provide notice of a security breach to a consumer by one or more of the following methods:

(A) Direct notice, which may be by one of the following methods:

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

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

(I) the data collector'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

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

(B)(i) Substitute notice, if:

(I) the data collector demonstrates that the lowest cost of providing notice to affected consumers pursuant to subdivision (6)(A) of this subsection among written, e-mail, or telephonic notice ~~to affected consumers~~ would exceed ~~$5,000.00~~ $10,000.00; or

(II) ~~the class of affected consumers to be provided written or telephonic notice exceeds 5,000; or~~

~~(III)~~ the data collector does not have sufficient contact information.

(ii) A data collector shall provide substitute notice by:

(I) conspicuously posting the notice on the data collector's website if the data collector maintains one; and

(II) notifying major statewide and regional media.

(c) In the event a data collector provides notice to more than 1,000 consumers at one time pursuant to this section, the data collector shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice. This subsection shall not apply to a person who is licensed or registered under Title 8 by the Department of Financial Regulation.

(d)(1) Notice of a security breach pursuant to subsection (b) of this section is not required if the data collector establishes that misuse of personal information is not reasonably possible and the data collector provides notice of the determination that the misuse of the personal information is not reasonably possible pursuant to the requirements of this subsection (d). If the data collector establishes that misuse of the personal information is not reasonably

possible, the data collector shall provide notice of its determination that misuse of the personal information is not reasonably possible and a detailed explanation for said determination to the Vermont Attorney General or to the Department of Financial Regulation in the event that the data collector is a person or entity licensed or registered with the Department under Title 8 or this title. The data collector may designate its notice and detailed explanation to the Vermont Attorney General or the Department of Financial Regulation as "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 collector established that misuse of personal information was not reasonably possible under subdivision (1) of this subsection (d), and subsequently obtains facts indicating that misuse of the personal information has occurred or is occurring, the data collector shall provide notice of the security breach pursuant to subsection (b) of this section.

(3) If a security breach is limited to an unauthorized acquisition of personally identifiable information comprising a consumer's name or Social Security number and login credentials, as specified in subdivision 2430(9)(A)(viii) of this title, for an online account other than an email account:

(A) the data collector shall provide notice of the security breach to the consumer electronically [*or by another reasonable method? – specify?]* and shall advise the consumer to take steps necessary to protect the online

account, including to change his or her login credentials for the account and for any other account for which the consumer uses the same login credentials; and

(B) if the personally identifiable information was acquired directly from the data collector [or its agent], the data collector shall provide notice of the security breach to the Attorney General or Department of Financial Regulation, as applicable.

(4) If a security breach is limited to an unauthorized acquisition of personally identifiable information comprising a consumer's name or Social Security number and login credentials, as specified in subdivision 2430(9)(A)(viii) of this title, for an email account:

(A) the data collector shall not provide notice of the security breach through the email account; and

(B) the data collector shall provide notice of the security breach *[through another reasonable method? -specify?]*, including [by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the {online account?} from an Internet protocol address or online location from which the data collector knows the consumer customarily accesses {the account}]

* * *

* * * Student Data Privacy * * *

Sec. 4. 9 V.S.A. chapter 62, subchapter 3A is added to read:

Subchapter 3A: Student Privacy

§ 2443. DEFINITIONS

As used in this subchapter:

(1) "Covered information" means personal information or material, or information that is linked to personal information or material, in any media or format that is:

(A)(i) not publicly available; or

(ii) made publicly available pursuant to the federal Family Educational and Rights and Privacy Act; and

(B)(i) created by or provided to an operator by a student or the student's parent or legal guardian in the course of the student's, parent's, or legal guardian's use of the operator's site, service, or application for PreK–12 school purposes;

(ii) created by or provided to an operator by an employee or agent of a school or school district for PreK–12 school purposes; or

(iii) gathered by an operator through the operation of its site, service, or application for PreK–12 school purposes and personally identifies a student, including information in the student's education record or electronic mail; first and last name; home address; telephone number; electronic mail

address or other information that allows physical or online contact; discipline records; test results; special education data; juvenile dependency records; grades; evaluations; criminal records; medical records; health records; social security number; biometric information; disability status; socioeconomic information; food purchases; political affiliations; religious information; text messages; documents; student identifiers; search activity; photos; voice recordings; or geolocation information.

(2) "PreK–12 school purposes" means purposes that are directed by or that customarily take place at the direction of a school, teacher, or school district; aid in the administration of school activities, including instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents; or are otherwise for the use and benefit of the school.

(3) "Operator" means, to the extent that an entity is operating in this capacity, the operator of an Internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for PreK–12 school purposes and was designed and marketed for PreK–12 school purposes.

(4) "School" means:

(A) a public or private preschool, kindergarten, elementary or secondary educational institution, vocational school, special educational agency or institution; and

(B) a person, agency, or institution that maintains school student records from more than one of the entities described in subdivision (6)(A) of this section.

(5) "Targeted advertising" means presenting advertisements to a student where the advertisement is selected based on information obtained or inferred over time from that student's online behavior, usage of applications, or covered information. The term does not include advertising to a student at an online location based upon that student's current visit to that location or in response to that student's request for information or feedback, without the retention of that student's online activities or requests over time for the purpose in whole or in part of targeting subsequent ads.

§ 2443a. OPERATOR PROHIBITIONS

(a) An operator shall not knowingly do any of the following with respect to its site, service, or application:

(1) Engage in targeted advertising on the operator's site, service, or application or target advertising on any other site, service, or application if the targeting of the advertising is based on any information, including covered information and persistent unique identifiers, that the operator has acquired

because of the use of that operator's site, service, or application for PreK–12 school purposes;

(2) Use information, including a persistent unique identifier, that is created or gathered by the operator's site, service, or application to amass a profile about a student, except in furtherance of PreK–12 school purposes. "Amass a profile" does not include the collection and retention of account information that remains under the control of the student, the student's parent or legal guardian, or the school.

(3) Sell, barter, or rent a student's information, including covered information. This subdivision (3) does not apply to the purchase, merger, or other type of acquisition of an operator by another entity if the operator or successor entity complies with this subchapter regarding previously acquired student information.

(4) Except as otherwise provided in section 2443c of this title, disclose covered information, unless the disclosure is made for one or more of the following purposes and is proportionate to the identifiable information necessary to accomplish the purpose:

(A) to further the PreK–12 school purposes of the site, service, or application, provided:

(i) the recipient of the covered information does not further disclose the information except to allow or improve operability and functionality of the operator's site, service, or application; and

(ii) the covered information is not used for a purpose inconsistent with this subchapter;

(B) to ensure legal and regulatory compliance or take precautions against liability;

(C) to respond to judicial process;

(D) to protect the safety or integrity of users of the site or others or the security of the site, service, or application;

(E) for a school, educational, or employment purpose requested by the student or the student's parent or legal guardian, provided that the information is not used or further disclosed for any other purpose; or

(F) to a third party if the operator contractually prohibits the third party from using any covered information for any purpose other than providing the contracted service to or on behalf of the operator, prohibits the third party from disclosing any covered information provided by the operator to subsequent third parties, and requires the third party to implement and maintain reasonable security procedures and practices.

(b) This section does not prohibit an operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application.

§ 2443b. OPERATOR DUTIES

An operator shall:

(1) implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information and designed to protect that covered information from unauthorized access, destruction, use, modification, or disclosure;

(2) delete, within a reasonable time period and to the extent practicable, a student's covered information if the school or school district requests deletion of covered information under the control of the school or school district, unless a student or his or her parent or legal guardian consents to the maintenance of the covered information; and

(3) publicly disclose and provide the school with material information about its collection, use, and disclosure of covered information, including publishing a term of service agreement, privacy policy, or similar document.

§ 2443c. PERMISSIVE USE OR DISCLOSURE

An operator may use or disclose covered information of a student under the following circumstances:

(1) if other provisions of federal or State law require the operator to disclose the information and the operator complies with the requirements of federal and State law in protecting and disclosing that information;

(2) for legitimate research purposes as required by State or federal law and subject to the restrictions under applicable State and federal law or as allowed by State or federal law and under the direction of a school, school district, or the State Board of Education if the covered information is not used for advertising or to amass a profile on the student for purposes other than for PreK–12 school purposes; and

(3) disclosure to a State or local educational agency, including schools and school districts, for PreK–12 school purposes as permitted by State or federal law.

§ 2443d. OPERATOR ACTIONS THAT ARE NOT PROHIBITED

This subchapter does not prohibit an operator from doing any of the following:

(1) using covered information to improve educational products if that information is not associated with an identified student within the operator's site, service, or application or other sites, services, or applications owned by the operator;

(2) using covered information that is not associated with an identified student to demonstrate the effectiveness of the operator's products or services, including in their marketing;

(3) sharing covered information that is not associated with an identified student for the development and improvement of educational sites, services, or applications;

(4) using recommendation engines to recommend to a student either of the following:

(A) additional content relating to an educational, other learning, or employment opportunity purpose within an online site, service, or application if the recommendation is not determined in whole or in part by payment or other consideration from a third party; or

(B) additional services relating to an educational, other learning, or employment opportunity purpose within an online site, service, or application if the recommendation is not determined in whole or in part by payment or other consideration from a third party; and

(5) responding to a student's request for information or for feedback without the information or response being determined in whole or in part by payment or other consideration from a third party.

§ 2443e. APPLICABILITY

This subchapter does not:

(1) limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or under a court order;

(2) limit the ability of an operator to use student data, including covered information, for adaptive learning or customized student learning purposes;

(3) apply to general audience Internet websites, general audience online services, general audience online applications, or general audience mobile applications, even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications;

(4) limit service providers from providing Internet connectivity to schools or students and their families;

(5) prohibit an operator of an Internet website, online service, online application, or mobile application from marketing educational products directly to parents if the marketing did not result from the use of covered information obtained by the operator through the provision of services covered under this subchapter;

(6) impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this subchapter on those applications or software;

(7) impose a duty upon a provider of an interactive computer service, as defined in 47 U.S.C. § 230, to review or enforce compliance with this subchapter by third-party content providers;

(8) prohibit students from downloading, exporting, transferring, saving, or maintaining their own student-created data or documents; or

(9) supersede the federal Family Educational Rights and Privacy Act or rules adopted pursuant to that Act.

§ 2443f. ENFORCEMENT

A person who violates a provision of this subchapter commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

Sec. 5. STUDENT PRIVACY; REVIEW; RECOMMENDATIONS

The Attorney General, in consultation with the Agency of Education, shall examine the issue of student data privacy as it relates to the federal Family Educational Rights and Privacy Act and access to student data by data brokers, and shall confer with parties of interest to determine any necessary recommendations.

* * * Effective Date * * *

Sec. 6. EFFECTIVE DATE

This act shall take effect on July 1, 2019.

(Committee vote: _____)

_____

Representative _____

FOR THE COMMITTEE