S.110

Introduced by Senators Sirotkin, Balint, Baruth, Clarkson and Hardy

Referred to Committee on Econ. Dev., Housing and General Affairs

Date: February 19, 2019

Subject: Commerce and trade; consumer protection

Statement of purpose of bill as introduced: This bill proposes to create a chief privacy officer; to direct the State to conduct a privacy audit concerning the collection and use of citizens' data; to adopt a student online privacy protection act; to expand the definition of personally identifiable information subject to the Security Breach Notice Act and ensure consumer notice of a data breach; and to require internet service providers to provide notice concerning the potential sharing of private data.

An act relating to data privacy and consumer protection

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

Sec. 1. CHIEF PRIVACY OFFICER

The Attorney General shall designate a current employee as Chief Privacy Officer for the State of Vermont and shall specify the duties of the position, which shall include responsibility for:

(1) ensuring that the State complies with privacy obligations and protects the privacy of its citizens through:

(A) training State employees;

(B) reviewing contracts to ensure that vendors are protecting citizen data; and

(C) considering the privacy implications of new programs and technologies;

(2) providing education and outreach to help citizens better protect themselves;

(3) advocating within the Executive and Legislative Branches concerning further protections for Vermonters, including amending existing law and recommending areas where data need not be collected; and

(4) serving as an ombudsman to hear citizen concerns regarding privacy issues.

Sec. 2. PRIVACY AUDIT

On or before January 15, 2020, the Chief Privacy Officer shall conduct a privacy audit and submit 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 a report concerning how the State of Vermont acquires and uses citizen data, including:

(1) which State government actors collect citizen data;

(2) what data they collect and whether it is publicly available;

(3) how they use the data;

(4) to whom they convey the data; and

(5) the purposes for which the recipients use the data.

Sec. 3. 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 in combination with any one or more of the following digital data elements, when either the name 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;

(ii) motor vehicle operator's license number or nondriver identification card number;

(iii) 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) account passwords or personal identification numbers or other access codes for a financial account;

(v) biometric information, including a finger print, retina scan, and facial recognition data;

(vi) genetic information;

(vii) health information;

(viii) login credentials, including a username or password; and

(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. 4. 9 V.S.A. § 2432 is added to read:

§ 2432. STUDENT ONLINE PRIVACY PROTECTION

(a) As used in this section:

(1) "Covered information" means personal information or materials, in any media or format, that meets one or more of the following:

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

(B) is created or provided by an employee or agent of the K–12 school, school district, local education agency, or county office of education to an operator; and

(C) is gathered by an operator through the operation of a website, service, or application described in subdivision (4) of this subsection (a) and is

descriptive of a student or otherwise identifies a student, including information in the student's educational record or e-mail, first and last name, home address, telephone number, e-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, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

(2) "K–12 school purposes" means purposes that customarily take place at the direction of the K–12 school, teacher, or school district or 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 for the use and benefit of the school.

(3) "Online service" includes cloud computing services, which shall comply with this section if they otherwise meet the definition of an operator.

(4) "Operator" means 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 K–12 purposes and is designed and marketed for K–12 purposes.

(b) An operator shall not knowingly engage in any of the following activities with respect to its site, service, or application:

(1)(A) target advertising on the operator's site, service, or application; or

(B) target advertising on any other site, service, or application when the targeting of the advertising is based upon information, including covered information and persistent unique identifiers, that the operator acquired because a consumer used the operator's website, service, or application.

(2) Use information, including persistent unique identifiers, created or gathered by the operator's website, service, or application, to amass a profile about a K–12 student except in furtherance of K–12 school purposes.

(3) Sell a student's information, including covered information. This prohibition does not apply to the purchase, merger, or other type of acquisition of an operator by another entity, provided that the operator or successor entity continues to be subject to the provisions of this section with respect to previously acquired student information.

(4) Disclose covered information unless the disclosure is made:

(A) in furtherance of the K–12 purpose of the website, service, or application, provided the recipient of the covered information disclosed pursuant to this subdivision (4):

(i) shall not further disclose the information unless done to allow or improve operability and functionality within that student's classroom or school; and

(ii) is legally required to comply with subsection (d) of this section;

(B) to ensure legal and regulatory compliance;

(C) to respond to or participate in judicial process;

(D) to protect the safety of users or others or security of the site; or

(E) to a service provider, provided the operator contractually:

(i) prohibits the service provider from using any covered information for any purpose other than providing the contracted service to, or on behalf of, the operator;

(ii) prohibits the service provider from disclosing any covered information provided by the operator with subsequent third parties; and

(iii) requires the service provider to implement and maintain reasonable security procedures and practices as provided in subsection (d) of this section.

(c) Nothing in subsection (b) of this section shall be construed to prohibit the operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's website, service, or application.

(d) An operator shall:

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

(2) delete a student's covered information if the school or district requests deletion of data under the control of the school or district.

(e) Notwithstanding subdivision (b)(4) of this section, an operator may disclose covered information of a student, as long as subdivisions (b)(1)–(3) are not violated, 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; and

(2) for legitimate research purposes:

(A) as required by State or federal law and subject to the restrictions under applicable State and federal law; or

(B) as allowed by State or federal law and under the direction of a school, school district, or state department of education, if no covered information is used for any purpose in furtherance of advertising or to amass a profile on the student for purposes other than K–12 school purposes; and

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

(f) Nothing in this section prohibits an operator from using deidentified student covered information as follows:

(1) within the operator's website, service, or application or other websites, services, or applications owned by the operator to improve educational products; or

(2) to demonstrate the effectiveness of the operator's products or services, including in their marketing.

(g) Nothing in this section prohibits an operator from sharing aggregated deidentified student covered information for the development and improvement of educational sites, services, or applications.

(h) This section shall not be construed to limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

(i) This section does not limit the ability of an operator to use student data, including covered information, for adaptive learning or customized student learning purposes.

(j) This section does not 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 website, service, or application may be used to access those general audience websites, services, or applications.

(k) This section does not limit Internet service providers from providing Internet connectivity to schools or students and their families.

(l) This section shall not be construed to prohibit an operator of an Internet website, online service, online application, or mobile application from marketing educational products directly to parents so long as the marketing did not result from the use of covered information obtained by the operator through the provision of services covered under this section.

(m) This section does not 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 section on those applications or software.

(n) This section does not 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 section by third-party content providers.

(o) This section does not impede the ability of students to download, export, or otherwise save or maintain their own student-created data or documents.

(p) A person who violates this section commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

Sec. 5. 9 V.S.A. § 2433 is added to read:

§ 2433. INTERNET SERVICE PROVIDERS; PRIVACY; DISCLOSURE

(a) A person who offers or provides Internet access service in this State shall, prior to executing a contract for service and annually thereafter:

(1) disclose to a consumer in writing whether the provider shares data it collects about the consumer with third parties; and

(2) if the provider shares data it collects about the consumer without first obtaining the consumer's prior consent, notify the consumer of that practice in bold and highlighted text.

(b) A person who violates this section commits an unfair and deceptive act in commerce in violation of section 2453 of this title.

Sec. 6. 9 V.S.A. § 2435(b)(6) is amended to read:

(6) A data collector ~~may~~ shall provide direct 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)~~(A) written notice mailed to the consumer's residence;

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

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

~~(iii)~~(C) 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 cost of providing written or telephonic notice to affected consumers would exceed $5,000.00;~~

~~(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.~~

Sec. 7. EFFECTIVE DATE

~~This act shall take effect on July 1, 2019.~~

Sec. 1. PRIVACY AUDIT

On or before January 15, 2020, the Chief Data Officer and the Chief Records Officer shall submit 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 a report concerning the three branches of State government and the management of personally identifiable information, as defined in 9 V.S.A. § 2430(9), as well as 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.

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 in combination with any one or more of the following digital data elements, when either the name 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;

(ii) motor vehicle operator's license number or nondriver identification card number;

(iii) 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) account passwords or personal identification numbers or other access codes 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;

(viii) login credentials, including a username or password; and

(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. 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 ~~K–12 school purposes~~ PreK–12 school purposes;

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

(iii) gathered by an operator through the operation of its site, service, or application for ~~K–12 school purposes~~ 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) ~~"K–12 school purposes"~~ "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 ~~K–12 school purposes~~ PreK–12 school purposes and was designed and marketed for ~~K–12 school purposes~~ PreK–12 school purposes.

(4) "School" means:

(A) a public or private preschool, ~~public~~ 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 ~~K–12 school purposes~~ 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 ~~K–12 school purposes~~ 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 ~~K–12 purposes~~ 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 ~~K–12 school purposes~~ PreK–12 school purposes; and

(3) disclosure to a State or local educational agency, including schools and school districts, for ~~K–12 school purposes~~ 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)*~~ *(5) 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)*~~ *(6) 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)*~~ *(7) prohibit students from downloading, exporting, transferring, saving, or maintaining their own student-created data or documents; or*

~~*(9)*~~ *(8) 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. 4. 9 V.S.A. § 2435(b)(6) is amended to read:

(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.

Sec. 5. EFFECTIVE DATE

This act shall take effect on July 1, 2019.