S.110

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

Referred to Committee on

Date:

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.