

1 Introduced by Senator Sirotkin

2 Referred to Committee on

3 Date:

4 Subject: Commerce and trade; consumer protection

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

12 An act relating to data privacy and consumer protection

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

14 Sec. 1. CHIEF PRIVACY OFFICER

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

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

20 (A) training State employees;

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

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

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

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

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

12           Sec. 2. PRIVACY AUDIT

13           On or before January 15, 2020, the Chief Privacy Officer shall conduct a  
14           privacy audit and submit to the House Committees on Commerce and  
15           Economic Development and on Government Operations and to the Senate  
16           Committees on Economic Development, Housing and General Affairs and on  
17           Government Operations a report concerning how the State of Vermont  
18           acquires and uses citizen data, including:

19           (1) which State government actors collect citizen data;

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

21           (3) how they use the data;

1           (4) to whom they convey the data; and

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

3           Sec. 3. 9 V.S.A. § 2430(9) is amended to read:

4           (9)(A) “Personally identifiable information” means a consumer’s first  
5           name or first initial and last name in combination with any one or more of the  
6           following digital data elements, when either the name or the data elements are  
7           not encrypted or redacted or protected by another method that renders them  
8           unreadable or unusable by unauthorized persons:

9                   (i) Social Security number;

10                   (ii) motor vehicle operator’s license number or nondriver  
11           identification card number;

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

15                   (iv) account passwords or personal identification numbers or other  
16           access codes for a financial account;

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

19                   (vi) genetic information;

20                   (vii) health information;

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

1                    (ix) a passport number.

2                    (B) “Personally identifiable information” does not mean publicly  
3 available information that is lawfully made available to the general public from  
4 federal, State, or local government records.

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

6                    § 2432. STUDENT ONLINE PRIVACY PROTECTION

7                    (a) As used in this section:

8                    (1) “Covered information” means personal information or materials, in  
9 any media or format, that meets on or more of the following:

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

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

17                    (C) is gathered by an operator through the operation of a website,  
18 service, or application described in subdivision (4) of this subsection (a) and is  
19 descriptive of a student or otherwise identifies a student, including information  
20 in the student’s educational record or e-mail, first and last name, home address,  
21 telephone number, e-mail address, or other information that allows physical or

1 online contact, discipline records, test results, special education data, juvenile  
2 dependency records, grades, evaluations, criminal records, medical records,  
3 health records, Social Security number, biometric information, disabilities,  
4 socioeconomic information, food purchases, political affiliations, religious  
5 information, text messages, documents, student identifiers, search activity,  
6 photos, voice recordings, or geolocation information.

7 (2) “K–12 school purposes” means purposes that customarily take place  
8 at the direction of the K–12 school, teacher, or school district or aid in the  
9 administration of school activities, including instruction in the classroom or at  
10 home, administrative activities, and collaboration between students, school  
11 personnel, or parents, or are for the use and benefit of the school.

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

14 (4) “Operator” means the operator of an Internet website, online service,  
15 online application, or mobile application with actual knowledge that the site,  
16 service, or application is used primarily for K–12 purposes and is designed and  
17 marketed for K–12 purposes.

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

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

21 or

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

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

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

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

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

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

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

1           (B) to ensure legal and regulatory compliance;

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

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

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

5                 (i) prohibits the service provider from using any covered

6 information for any purpose other than providing the contracted service to, or

7 on behalf of, the operator;

8                 (ii) prohibits the service provider from disclosing any covered

9 information provided by the operator with subsequent third parties; and

10                (iii) requires the service provider to implement and maintain

11 reasonable security procedures and practices as provided in subsection (d) of

12 this section.

13           (c) Nothing in subsection (b) of this section shall be construed to prohibit

14 the operator's use of information for maintaining, developing, supporting,

15 improving, or diagnosing the operator's website, service, or application.

16           (d) An operator shall:

17                 (1) implement and maintain reasonable security procedures and

18 practices appropriate to the nature of the covered information, and protect that

19 information from unauthorized access, destruction, use, modification, or

20 disclosure; and

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

3           (e) Notwithstanding subdivision (b)(4) of this section, an operator may  
4           disclose covered information of a student, as long as subdivisions (b)(1)–(3)  
5           are not violated, under the following circumstances:

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

9           (2) for legitimate research purposes:

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

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

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

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

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

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

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

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

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

15           (j) This section does not apply to general audience Internet websites,  
16           general audience online services, general audience online applications, or  
17           general audience mobile applications, even if login credentials created for an  
18           operator’s website, service, or application may be used to access those general  
19           audience websites, services, or applications.

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

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

6        (m) This section does not impose a duty upon a provider of an electronic  
7        store, gateway, marketplace, or other means of purchasing or downloading  
8        software or applications to review or enforce compliance of this section on  
9        those applications or software.

10       (n) This section does not impose a duty upon a provider of an interactive  
11       computer service, as defined in 47 U.S.C. § 230, to review or enforce  
12       compliance with this section by third-party content providers.

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

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

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

19       § 2433. INTERNET SERVICE PROVIDERS; PRIVACY; DISCLOSURE

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

1           (1) disclose to a consumer in writing its data privacy practices, including  
2           what data the provider may collect about the consumer, to whom it may be  
3           disclosed and for what purposes, and whether the consumer has the right to opt  
4           out of data sharing; and

5           (2) obtain acknowledgment from the consumer that he or she has  
6           received a disclosure of the service provider’s data privacy practices and that  
7           he or she accepts the terms and conditions of use, specifically including the  
8           terms and conditions applicable to data sharing.

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

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

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

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

15           ~~(i)(A)~~ written notice mailed to the consumer’s residence;

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

18           ~~(i)~~ the data collector’s primary method of communication  
19           with the consumer is by electronic means, the electronic notice does not  
20           request or contain a hypertext link to a request that the consumer provide  
21           personal information, and the electronic notice conspicuously warns consumers

1 not to provide personal information in response to electronic communications  
2 regarding security breaches; or

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

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

7 ~~(B)~~(i) ~~Substitute notice, if:~~

8 ~~(I) the data collector demonstrates that the cost of providing~~  
9 ~~written or telephonic notice to affected consumers would exceed \$5,000.00;~~

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

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

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

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

17 ~~(II) notifying major statewide and regional media.~~

18 Sec. 7. EFFECTIVE DATE

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