

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 Secretary of Digital Services shall designate a current employee as  
16 Chief Privacy Officer for the State of Vermont and shall specify the duties of  
17 the position, 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; and

5           (D) other duties that the Secretary in his or her discretion determines  
6           are appropriate to protect citizens' privacy;

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

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

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

14          Sec. 2. PRIVACY AUDIT

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

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

- 1           (2) what data they collect and whether it is publicly available;
- 2           (3) how they use the data;
- 3           (4) to whom they convey the data;
- 4           (5) the purposes for which the recipients use the data;
- 5           (6) revenue impacts; and
- 6           (7) a survey of federal and State statutes and rules that require data
- 7           collection.

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

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

14                   (i) Social Security number;

15                   (ii) motor vehicle operator’s license number or nondriver  
16           identification card number;

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

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

1                   (v) biometric information, including a finger print, retina scan, and  
2 facial recognition data; [further refine?]

3                   (vi) genetic information;

4                   (vii) health information;

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

6                   (ix) a passport number.

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

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

11                   § 2432. STUDENT ONLINE PRIVACY PROTECTION

12                   (a) As used in this section:

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

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

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

1           (C) is gathered by an operator through the operation of a website,  
2           service, or application described in subdivision (4) of this subsection (a) and is  
3           descriptive of a student or otherwise identifies a student, including information  
4           in the student’s educational record or e-mail, first and last name, home address,  
5           telephone number, e-mail address, or other information that allows physical or  
6           online contact, discipline records, test results, special education data, juvenile  
7           dependency records, grades, evaluations, criminal records, medical records,  
8           health records, Social Security number, biometric information, disabilities,  
9           socioeconomic information, food purchases, political affiliations, religious  
10           information, text messages, documents, student identifiers, search activity,  
11           photos, voice recordings, or geolocation information.

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

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

19           (4) “Operator” means the operator of an Internet website, online service,  
20           online application, or mobile application with actual knowledge that the site,

1 service, or application is used primarily for K–12 purposes and is designed and  
2 marketed for K–12 purposes.

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

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

6 or

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

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

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

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

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

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

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

9                   (B) to ensure legal and regulatory compliance;

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

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

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

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

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

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

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

4        (d) An operator shall:

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

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

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

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

17            (2) for legitimate research purposes:

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

20            (B) as allowed by State or federal law and under the direction of a  
21            school, school district, or state department of education, if no covered



1 information is used for any purpose in furtherance of advertising or to amass a  
2 profile on the student for purposes other than K–12 school purposes; and

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

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

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

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

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

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

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

1        (j) This section does not apply to general audience Internet websites,  
2        general audience online services, general audience online applications, or  
3        general audience mobile applications, even if login credentials created for an  
4        operator’s website, service, or application may be used to access those general  
5        audience websites, services, or applications.

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

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

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

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

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

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

6                   \* \* \* “Compromise Version” of SOIPA \* \* \*

7                   CHAPTER 134: STUDENT PRIVACY

8       §4032. DEFINITIONS

9       As used in this Chapter:

10       (1) “Covered information” means personal information or material **or**  
11       **information that is linked to personal information or material** in any media or  
12       **format that is not publicly available (other than information that is publicly**  
13       **available by virtue of having been disclosed under FERPA)** and is any of the  
14       following:

15       (a) Created by or provided to an operator by a student or the student’s  
16       parent or legal guardian in the course of the student’s, parent’s, or legal  
17       guardian’s use of the operator’s site, service, or application for K-12 school  
18       purposes.

19       (b) Created by or provided to an operator by an employee or agent of a  
20       school or school district for K-12 school purposes.

1     (c) Gathered by an operator through the operation of its site, service, or  
2     application for K-12 school purposes and ~~is descriptive of a student or~~  
3     ~~otherwise identifies a student~~ personally identifies a student, including, but not  
4     limited to, information in the student’s educational record or electronic mail,  
5     first and last name, home address, telephone number, electronic mail address,  
6     or other information that allows physical or online contact, discipline records,  
7     test results, special education data, juvenile dependency records, grades,  
8     evaluations, criminal records, medical records, health records, a social security  
9     number, biometric information, disabilities, socioeconomic information, food  
10    purchases, political affiliations, religious information, text messages,  
11    documents, student identifiers, search activity, photos, voice recordings, or  
12    geolocation information.

13    (2) “Disclosable directory information” means with respect to a student, the  
14    student’s name; photograph; age (other than exact date of birth); major field of  
15    study; grade level; enrollment status (e.g., undergraduate or graduate, full-time  
16    or part-time); dates of attendance; participation in officially recognized  
17    activities and sports; weight and height of members of athletic teams; degrees,  
18    honors and awards received; and the most recent educational agency or  
19    institution attended.

1 (3) “Interactive computer service” has the meaning ascribed to that term in  
2 Section 230 of the federal Communications Decency Act of 1996 (47 U.S.C.  
3 230). [this definition is unnecessary – defined later and term used only once]

4 (4) “K-12 school purposes” means purposes that are directed by or that  
5 customarily take place at the direction of a school, teacher, or school district;  
6 aid in the administration of school activities, including, but not limited to,  
7 instruction in the classroom or at home, administrative activities, and  
8 collaboration between students, school personnel, or parents; or are otherwise  
9 for the use and benefit of the school.

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

12 (5) “Operator” means, to the extent that an entity is operating in this capacity,  
13 the operator of an Internet website, online service, online application, or  
14 mobile application with actual knowledge that the site, service, or application  
15 is used primarily for K-12 school purposes and was designed and marketed for  
16 K-12 school purposes.

17 (6) “School” means (1) any preschool, public kindergarten, elementary or  
18 secondary educational institution, vocational school, special educational  
19 agency or institution or (2) any person, agency, or institution that maintains  
20 school student records from more than one school. “School” includes a private  
21 or nonpublic school.

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

9 (8) “Student”, “directory information”, and “eligible student”, have the same  
10 meaning as in 34 Code of Federal Regulations Part 99.

11 § 4033. OPERATOR PROHIBITIONS

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

14 (1) Engage in targeted advertising on the operator’s site, service, or application  
15 or target advertising on any other site, service, or application if the targeting of  
16 the advertising is based on any information, including covered information and  
17 persistent unique identifiers, that the operator has acquired because of the use  
18 of that operator’s site, service, or application for K-12 school purposes.

19 (2) Use information, including persistent unique identifiers, created or gathered  
20 by the operator’s site, service, or application to amass a profile about a K-12  
21 student, except in furtherance of K-12 school purposes. “Amass a profile” does

1 not include the collection and retention of account information that remains  
2 under the control of the student, the student's parent or legal guardian, or the  
3 school.

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

8 (4) Except as otherwise provided in §4035 of this Act, disclose covered  
9 information, unless the disclosure is made for the following purposes :and is  
10 proportionate to the identifiable information necessary to accomplish the  
11 purpose:

12 (a) In furtherance of the K-12 purposes of the site, service, or  
13 application if the recipient of the covered information disclosed under this  
14 clause (a) does not further disclose the information, unless done to allow or  
15 improve operability and functionality within that student's classroom or school  
16 and [the recipient] is legally required to comply with subsection (d) of this  
17 section; of the operator's site, service, or application and is not used for  
18 purpose inconsistent with this Act.

19 (b) To ensure legal and regulatory compliance or take precautions against  
20 liability.

21 (c) To respond or participate in to judicial process.

1 (d) To protect the safety or integrity of users of the site or others or the  
2 security of the site, service, or application.

3 (e) For a school, educational, or employment purpose requested by the  
4 student or the student’s parent or legal guardian, provided that the information  
5 is not used or further disclosed for any other purpose.

6 (f) To a ~~service provider~~ third party if the operator contractually prohibits  
7 the third party from using any covered information for any purpose other than  
8 providing the contracted service to or on behalf of the operator, prohibits the  
9 third party from disclosing any covered information provided by the operator  
10 to subsequent third parties, and requires the third party to implement and  
11 maintain reasonable security procedures and practices as provided in  
12 subsection (d) of this section.

13 Nothing in this section prohibits the operator’s use of information for  
14 maintaining, developing, supporting, improving, or diagnosing the operator’s  
15 site, service, or application.

#### 16 §4034. OPERATOR DUTIES

17 An operator shall do the following:

18 (1) Implement and maintain reasonable security procedures and practices  
19 appropriate to the nature of the covered information and designed to protect  
20 that covered information from unauthorized access, destruction, use,  
21 modification, or disclosure.



1 (2) Delete, within a reasonable time period and to the extent practicable, a  
2 student’s covered information if the school or school district requests deletion  
3 of data covered information under the control of the school or school district,  
4 unless a student or his or her parent or legal guardian consents to the  
5 maintenance of the covered information.

6 (3) Publicly disclose and provide the school with material information about  
7 its collection, use, and disclosure of covered information, including, but not  
8 limited to, publishing a term of service agreement, privacy policy, or similar  
9 document.

10 §4035. PERMISSIVE USE OR DISCLOSURE

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

13 (1) If other provisions of federal or State law require the operator to disclose  
14 the information, and the operator complies with the requirements of federal  
15 and State law in protecting and disclosing that information.

16 (2) For legitimate research purposes as required by State or federal law and  
17 subject to the restrictions under applicable State and federal law or as allowed  
18 by State or federal law and under the direction of a school, school district, or  
19 the State Board of Education if the covered information is not used for  
20 advertising or to amass a profile on the student for purposes other than for K-  
21 12 school purposes.

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

3 §4036. OPERATOR ACTIONS THAT ARE NOT PROHIBITED.

4 Nothing in this section prohibits an operator from using deidentified student  
5 covered information as follows:

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

7  
8 (1) Using covered information to improve educational products if that  
9 information is not associated with an identified student within the operator’s  
10 site, service, or application or other sites, services, or applications owned by  
11 the operator.

12 (2) Using covered information that is not associated with an identified student  
13 to demonstrate the effectiveness of the operator’s products or services,  
14 including in their marketing.

15 (3) Sharing aggregated deidentified student covered information that is not  
16 associated with an identified student for the development and improvement of  
17 educational sites, services, or applications.

18 (4) Using recommendation engines to recommend to a student either of the  
19 following:

20 (a) Additional content relating to an educational, other learning, or  
21 employment opportunity purpose within an online site, service, or application

1 if the recommendation is not determined in whole or in part by payment or  
2 other consideration from a third party.

3 (b) Additional services relating to an educational, other learning, or  
4 employment opportunity purpose within an online site, service, or application  
5 if the recommendation is not determined in whole or in part by payment or  
6 other consideration from a third party.

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

10 §4037. APPLICABILITY

11 §§4033-4036, inclusive, shall not do any of the following:

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

14 (2) Limit the ability of an operator to use student data, including covered  
15 information, for adaptive learning or customized student learning purposes.

16 (3) Apply to general audience Internet websites, general audience online  
17 services, general audience online applications, or general audience mobile  
18 applications, even if login credentials created for an operator’s site, service, or  
19 application may be used to access those general audience sites, services, or  
20 applications.

1 (4) Limit service providers from providing Internet connectivity to schools or  
2 students and their families.

3 (5) Prohibit an operator of an Internet website, online service, online  
4 application, or mobile application from marketing educational products  
5 directly to parents if the marketing did not result from the use of covered  
6 information obtained by the operator through the provision of services covered  
7 under this Act.

8 (6) Impose a duty upon a provider of an electronic store, gateway, marketplace,  
9 or other means of purchasing or downloading software or applications to  
10 review or enforce compliance with this Act on those applications or software.

11 (7) Impose a duty upon a provider of an interactive computer service as  
12 defined in Section 230 of Title 47 of the United States Code, to review or  
13 enforce compliance with this Act by third-party content providers.

14 (8) Prohibit students from downloading, exporting, transferring, saving, or  
15 maintaining their own student-created data or documents.

16 (9) Supersede the federal Family Educational Rights and Privacy Act of 1974  
17 or rules adopted pursuant to that Act.

18 § 4038. SCHOOL LIMITS ON DISCLOSURE OF DIRECTORY

19 INFORMATION AND COVERED INFORMATION

1 (1) A school shall disclose covered information about a student to the parent  
2 of the student or to the eligible student in accordance with applicable state and  
3 federal law.

4 (2) In addition to the uses allowed in §§4033 through 4036, inclusive, a school  
5 may disclose directory information about a student as provided in 34 Code of  
6 Federal Regulations Section 99.37 only:

7 (a) after giving the parent of the student or the eligible student  
8 at the school notice and an opportunity to opt-out of the disclosure in  
9 accordance with Section 4;

10 (b) such opportunity shall be available online on the website of  
11 the school, if the school has a website, for at least all days during the  
12 academic year; and

13 (c) the school shall offer the opportunity to allow a parent to  
14 opt-in to disclosure to a school newspaper; local newspaper; school  
15 club or organization; school yearbook; honor roll or other recognition  
16 list; graduation program; sports related publication which provides  
17 specific information about particular students for the purposes of a  
18 specific sports activity or function; or parent and teacher organization –  
19 while allowing the parent to opt out of other uses of directory  
20 information.

21 § 4039. NOTICE

1 (1) Within the first week of each school year, each school shall issue a public  
2 notice, include in a student or parent handbook, provide online in an easily  
3 accessible location, and provide to each student in a form that the student can  
4 retain or give to a parent, information describing the school's disclosure  
5 procedures for covered information.

6 (2) The information required under subsection (a) shall include:

7 (a) a description of any covered information that the school expects to  
8 disclose during the school year;

9 (b) the procedure that a parent of a student or an eligible student can follow  
10 to prohibit the school from disseminating disclosable directory information  
11 under section 3 of this Act; and

12 (c) the procedure that a parent of a student or an eligible student can follow  
13 to authorize the school to disseminate covered information.

14 (3) If the school does not receive an objection from the parent of a student or  
15 the eligible student within thirty days of the dissemination of the information  
16 required to be provided under subsection (a), the school may disseminate  
17 disclosable directory information relating to the student.

18 (4) The parent or eligible student may update this form at any time throughout  
19 the year., except for emergency circumstances including but not limited to the  
20 safety of the student.

21 §4040. ENFORCEMENT

1 Violations of this Act shall constitute unlawful practices for which the  
2 Attorney General may take appropriate action under the [VT UDAP Statute].

3 §4041. SEVERABILITY

4 The provisions of this Act are severable.

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

7 § 2433. INTERNET SERVICE PROVIDERS; PRIVACY; DISCLOSURE

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

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

14 (2) obtain acknowledgment from the consumer that he or she has  
15 received a disclosure of the service provider's data privacy practices and that  
16 he or she accepts the terms and conditions of use, specifically including the  
17 terms and conditions applicable to data sharing.

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

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

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

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

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

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

7           ~~(i)~~ (i) the data collector's primary method of communication  
8 with the consumer is by electronic means, the electronic notice does not  
9 request or contain a hypertext link to a request that the consumer provide  
10 personal information, and the electronic notice conspicuously warns consumers  
11 not to provide personal information in response to electronic communications  
12 regarding security breaches; or

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

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

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

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

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



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

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

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

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

7                   Sec. 7. EFFECTIVE DATE

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