

1 TO THE HOUSE OF REPRESENTATIVES:

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

7 \* \* \* Data Privacy; State Government \* \* \*

8 Sec. 1. DATA PRIVACY INVENTORY

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

15 (1) the State Court Administrator for the Judicial Branch;

16 (2) the Deputy Director for Information Technology within the Office of  
17 Legislative Council for the Legislative Branch; and

18 (3) the Chief Data Officer within the Agency of Digital Services and the  
19 Chief Records Officer within the Office of the Secretary of State for the  
20 Executive Branch.

1        (b) The inventory and report for each branch shall address the collection  
2        and management of personally identifiable information, as defined in 9 V.S.A.  
3        § 2430, and of street addresses, e-mail addresses, telephone numbers, and  
4        demographic information, specifically:

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

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

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

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

12                      (D) require personally identifiable information to be shared between  
13                      branches of State government or between branches and nonstate entities,  
14                      including municipalities;

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



1           (9) “Login credentials” means a consumer’s user name or e-mail  
2           address, in combination with a password or an answer to a security question,  
3           that together permit access to an online account.

4           ~~(9)(10)(A)~~ “Personally identifiable information” means a consumer’s  
5           first name or first initial and last name in combination with ~~any~~ one or more of  
6           the following digital data elements, when the data elements are not encrypted,  
7           ~~or~~ redacted, or protected by another method that renders them unreadable or  
8           unusable by unauthorized persons:

9                   (i) a Social Security number;

10                   (ii) ~~motor vehicle operator’s license number or nondriver~~  
11           ~~identification card number~~ a driver license or nondriver State identification  
12           card number, individual taxpayer identification number, passport number,  
13           military identification card number, or other identification number that  
14           originates from a government identification document that is commonly used  
15           to verify identity for a commercial transaction;

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

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

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

6                   (vi) genetic information; and

7                   (vii)(I) health records or records of a wellness program or similar  
8                   program of health promotion or disease prevention;

9                   (II) a health care professional’s medical diagnosis or treatment  
10                  of the consumer; or

11                  (III) a health insurance policy number.

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

15                  ~~(10)~~(11) “Record” means any material on which written, drawn, spoken,  
16                  visual, or electromagnetic information is recorded or preserved, regardless of  
17                  physical form or characteristics.

18                  ~~(11)~~(12) “Redaction” means the rendering of data so that the data are  
19                  unreadable or are truncated so that no more than the last four digits of the  
20                  identification number are accessible as part of the data.

1           ~~(12)~~(13)(A) “Security breach” means unauthorized acquisition of,  
2           electronic data or a reasonable belief of an unauthorized acquisition of,  
3           electronic data that compromises the security, confidentiality, or integrity of a  
4           consumer’s personally identifiable information or login credentials maintained  
5           by a data collector.

6           (B) “Security breach” does not include good faith but unauthorized  
7           acquisition of personally identifiable information or login credentials by an  
8           employee or agent of the data collector for a legitimate purpose of the data  
9           collector, provided that the personally identifiable information ~~is~~ or login  
10          credentials are not used for a purpose unrelated to the data collector’s business  
11          or subject to further unauthorized disclosure.

12          (C) In determining whether personally identifiable information ~~has~~ or  
13          login credentials have been acquired or is reasonably believed to have been  
14          acquired by a person without valid authorization, a data collector may consider  
15          the following factors, among others:

16                 (i) indications that the information is in the physical possession  
17                 and control of a person without valid authorization, such as a lost or stolen  
18                 computer or other device containing information;

19                 (ii) indications that the information has been downloaded or  
20                 copied;

1 (iii) indications that the information was used by an unauthorized  
2 person, such as fraudulent accounts opened or instances of identity theft  
3 reported; or

4 (iv) that the information has been made public.

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

6 § 2435. NOTICE OF SECURITY BREACHES

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

8 (b) Notice of breach.

9 (1) Except as ~~set forth~~ otherwise provided in subsection (d) of this  
10 section, any data collector that owns or licenses computerized personally  
11 identifiable information or login credentials ~~that includes personal information~~  
12 ~~concerning a consumer~~ shall notify the consumer that there has been a security  
13 breach following discovery or notification to the data collector of the breach.  
14 Notice of the security breach shall be made in the most expedient time possible  
15 and without unreasonable delay, but not later than 45 days after the discovery  
16 or notification, consistent with the legitimate needs of the law enforcement  
17 agency, as provided in subdivisions (3) and (4) of this subsection (b), or with  
18 any measures necessary to determine the scope of the security breach and  
19 restore the reasonable integrity, security, and confidentiality of the data system.

20 (2) Any data collector that maintains or possesses computerized data  
21 containing personally identifiable information ~~of a consumer~~ or login

1 credentials that the data collector does not own or license or any data collector  
2 that acts or conducts business in Vermont that maintains or possesses records  
3 or data containing personally identifiable information or login credentials that  
4 the data collector does not own or license shall notify the owner or licensee of  
5 the information of any security breach immediately following discovery of the  
6 breach, consistent with the legitimate needs of law enforcement as provided in  
7 subdivisions (3) and (4) of this subsection (b).

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

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

15 (B)(i) The data collector shall notify the Attorney General or the  
16 Department, as applicable, of the date of the security breach and the date of  
17 discovery of the breach and shall provide a preliminary description of the  
18 breach within 14 business days, consistent with the legitimate needs of the law  
19 enforcement agency as provided in this subdivision (3) and subdivision (4) of  
20 this subsection (b), of the data collector's discovery of the security breach or



1 when the data collector provides notice to consumers pursuant to this section,  
2 whichever is sooner.

3 (ii) Notwithstanding subdivision (B)(i) of this subdivision (b)(3), a  
4 data collector who, prior to the date of the breach, on a form and in a manner  
5 prescribed by the Attorney General, had sworn in writing to the Attorney  
6 General that it maintains written policies and procedures to maintain the  
7 security of personally identifiable information or login credentials and respond  
8 to a breach in a manner consistent with Vermont law shall notify the Attorney  
9 General of the date of the security breach and the date of discovery of the  
10 breach and shall provide a description of the breach prior to providing notice of  
11 the breach to consumers pursuant to subdivision (1) of this subsection (b).

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

16 (iv) Unless otherwise ordered by a court of this State for good  
17 cause shown, a notice provided under this subdivision (3)(B) shall not be  
18 disclosed to any person other than the Department, the authorized agent or  
19 representative of the Attorney General, a State's Attorney, or another law  
20 enforcement officer engaged in legitimate law enforcement activities without  
21 the consent of the data collector.

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

6           (ii) The data collector may send to the Attorney General or the  
7 Department, as applicable, a second copy of the consumer notice, from which  
8 is redacted the type of personally identifiable information or login credentials  
9 that was subject to the breach, and which the Attorney General or the  
10 Department shall use for any public disclosure of the breach.

11           (D) If a security breach is limited to an unauthorized acquisition of  
12 login credentials, a data collector is only required to provide notice of the  
13 security breach to the Attorney General or Department of Financial Regulation,  
14 as applicable, if the login credentials were acquired directly from the data  
15 collector or its agent.

16           (4)(A) The notice to a consumer required by this subsection shall be  
17 delayed upon request of a law enforcement agency. A law enforcement agency  
18 may request the delay if it believes that notification may impede a law  
19 enforcement investigation, or a national or Homeland Security investigation or  
20 jeopardize public safety or national or Homeland Security interests. In the  
21 event law enforcement makes the request for a delay in a manner other than in

1 writing, the data collector shall document such request contemporaneously in  
2 writing, including the name of the law enforcement officer making the request  
3 and the officer's law enforcement agency engaged in the investigation. A law  
4 enforcement agency shall promptly notify the data collector in writing when  
5 the law enforcement agency no longer believes that notification may impede a  
6 law enforcement investigation, or a national or Homeland Security  
7 investigation or jeopardize public safety or national or Homeland Security  
8 interests. The data collector shall provide notice required by this section  
9 without unreasonable delay upon receipt of a written communication, which  
10 includes facsimile or electronic communication, from the law enforcement  
11 agency withdrawing its request for delay.

12 (B) A Vermont law enforcement agency with a reasonable belief that  
13 a security breach has or may have occurred at a specific business shall notify  
14 the business in writing of its belief. The agency shall also notify the business  
15 that additional information on the security breach may need to be furnished to  
16 the Office of the Attorney General or the Department of Financial Regulation  
17 and shall include the website and telephone number for the Office and the  
18 Department in the notice required by this subdivision. Nothing in this  
19 subdivision shall alter the responsibilities of a data collector under this section  
20 or provide a cause of action against a law enforcement agency that fails,  
21 without bad faith, to provide the notice required by this subdivision.

1 (5) The notice to a consumer required in subdivision (1) of this  
2 subsection (b) shall be clear and conspicuous. ~~The~~ A notice to a consumer of a  
3 security breach involving personally identifiable information shall include a  
4 description of each of the following, if known to the data collector:

5 (A) the incident in general terms;

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

8 (C) the general acts of the data collector to protect the personally  
9 identifiable information from further security breach;

10 (D) a telephone number, toll-free if available, that the consumer may  
11 call for further information and assistance;

12 (E) advice that directs the consumer to remain vigilant by reviewing  
13 account statements and monitoring free credit reports; and

14 (F) the approximate date of the security breach.

15 (6) A data collector may provide notice of a security breach involving  
16 personally identifiable information to a consumer by one or more of the  
17 following methods:

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

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

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

1 (I) the data collector’s primary method of communication with  
2 the consumer is by electronic means, the electronic notice does not request or  
3 contain a hypertext link to a request that the consumer provide personal  
4 information, and the electronic notice conspicuously warns consumers not to  
5 provide personal information in response to electronic communications  
6 regarding security breaches; or

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

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

11 (B)(i) Substitute notice, if:

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

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

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

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

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

3 (II) notifying major statewide and regional media.

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

11 (d)(1) Notice of a security breach pursuant to subsection (b) of this section  
12 is not required if the data collector establishes that misuse of ~~personal~~  
13 ~~information~~ personally identifiable information or login credentials is not  
14 reasonably possible and the data collector provides notice of the determination  
15 that the misuse of the ~~personal information~~ personally identifiable information  
16 or login credentials is not reasonably possible pursuant to the requirements of  
17 this subsection (d). If the data collector establishes that misuse of the ~~personal~~  
18 ~~information~~ personally identifiable information or login credentials is not  
19 reasonably possible, the data collector shall provide notice of its determination  
20 that misuse of the ~~personal information~~ personally identifiable information or  
21 login credentials is not reasonably possible and a detailed explanation for said

1 determination to the Vermont Attorney General or to the Department of  
2 Financial Regulation in the event that the data collector is a person or entity  
3 licensed or registered with the Department under Title 8 or this title. The data  
4 collector may designate its notice and detailed explanation to the Vermont  
5 Attorney General or the Department of Financial Regulation as “trade secret”  
6 if the notice and detailed explanation meet the definition of trade secret  
7 contained in 1 V.S.A. § 317(c)(9).

8 (2) If a data collector established that misuse of ~~personal information~~  
9 personally identifiable information or login credentials was not reasonably  
10 possible under subdivision (1) of this subsection (d), and subsequently obtains  
11 facts indicating that misuse of the ~~personal information~~ personally identifiable  
12 information or login credentials has occurred or is occurring, the data collector  
13 shall provide notice of the security breach pursuant to subsection (b) of this  
14 section.

15 (3) If a security breach is limited to an unauthorized acquisition of login  
16 credentials for an online account other than an e-mail account the data  
17 collector shall provide notice of the security breach to the consumer  
18 electronically or through one or more of the methods specified in subdivision  
19 (b)(6) of this section and shall advise the consumer to take steps necessary to  
20 protect the online account, including to change his or her login credentials for

1 the account and for any other account for which the consumer uses the same  
2 login credentials.

3 (4) If a security breach is limited to an unauthorized acquisition of login  
4 credentials for an email account:

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

7 (B) the data collector shall provide notice of the security breach  
8 through one or more of the methods specified in subdivision (b)(6) of this  
9 section or by clear and conspicuous notice delivered to the consumer online  
10 when the consumer is connected to the online account from an Internet  
11 protocol address or online location from which the data collector knows the  
12 consumer customarily accesses the account.

13 (e) A data collector that is subject to the privacy, security, and breach  
14 notification rules adopted in 45 C.F.R. Part 164 pursuant to the federal Health  
15 Insurance Portability and Accountability Act, P.L. 104-191 (1996) is deemed  
16 to be in compliance with this subchapter if:

17 (1) the data collector experiences a security breach that is limited to  
18 personally identifiable information specified in 2430(10)(A)(vii); and

19 (2) the data collector provides notice to affected consumers pursuant  
20 to the requirements of the breach notification rule in 45 C.F.R. Part 164,  
21 Subpart D.



1        (f) Any waiver of the provisions of this subchapter is contrary to public  
2        policy and is void and unenforceable.

3        ~~(f)~~(g) Except as provided in subdivision (3) of this subsection (g), a  
4        financial institution that is subject to the following guidances, and any  
5        revisions, additions, or substitutions relating to an interagency guidance shall  
6        be exempt from this section:

7            (1) The Federal Interagency Guidance Response Programs for  
8        Unauthorized Access to Consumer Information and Customer Notice, issued  
9        on March 7, 2005, by the Board of Governors of the Federal Reserve System,  
10       the Federal Deposit Insurance Corporation, the Office of the Comptroller of  
11       the Currency, and the Office of Thrift Supervision.

12           (2) Final Guidance on Response Programs for Unauthorized Access to  
13       Member Information and Member Notice, issued on April 14, 2005, by the  
14       National Credit Union Administration.

15           (3) A financial institution regulated by the Department of Financial  
16       Regulation that is subject to subdivision (1) or (2) of this subsection ~~(f)~~(g) shall  
17       notify the Department as soon as possible after it becomes aware of an incident  
18       involving unauthorized access to or use of personally identifiable information.

19        ~~(g)~~(h) Enforcement.

20           (1) With respect to all data collectors and other entities subject to this  
21       subchapter, other than a person or entity licensed or registered with the

1 Department of Financial Regulation under Title 8 or this title, the Attorney  
2 General and State’s Attorney shall have sole and full authority to investigate  
3 potential violations of this subchapter and to enforce, prosecute, obtain, and  
4 impose remedies for a violation of this subchapter or any rules or regulations  
5 made pursuant to this chapter as the Attorney General and State’s Attorney  
6 have under chapter 63 of this title. The Attorney General may refer the matter  
7 to the State’s Attorney in an appropriate case. The Superior Courts shall have  
8 jurisdiction over any enforcement matter brought by the Attorney General or a  
9 State’s Attorney under this subsection.

10 (2) With respect to a data collector that is a person or entity licensed or  
11 registered with the Department of Financial Regulation under Title 8 or this  
12 title, the Department of Financial Regulation shall have the full authority to  
13 investigate potential violations of this subchapter and to prosecute, obtain, and  
14 impose remedies for a violation of this subchapter or any rules or regulations  
15 adopted pursuant to this subchapter, as the Department has under Title 8 or this  
16 title or any other applicable law or regulation.

17 \* \* \* Student Data Privacy \* \* \*

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

19 Subchapter 3A: Student Privacy

20 § 2443. DEFINITIONS

21 As used in this subchapter:

1           (1) “Covered information” means personal information or material, or  
2           information that is linked to personal information or material, in any media or  
3           format that is:

4                   (A)(i) not publicly available; or

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

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

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

13                   (iii) gathered by an operator through the operation of its site,  
14           service, or application for PreK–12 school purposes and personally identifies a  
15           student, including information in the student’s education record or electronic  
16           mail; first and last name; home address; telephone number; electronic mail  
17           address or other information that allows physical or online contact; discipline  
18           records; test results; special education data; juvenile dependency records;  
19           grades; evaluations; criminal records; medical records; health records; social  
20           security number; biometric information; disability status; socioeconomic  
21           information; food purchases; political affiliations; religious information; text

1 messages; documents; student identifiers; search activity; photos; voice  
2 recordings; or geolocation information.

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

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

14 (4) “School” means:

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

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

1           (5) “Targeted advertising” means presenting advertisements to a student  
2           where the advertisement is selected based on information obtained or inferred  
3           over 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           § 2443a. OPERATOR PROHIBITIONS

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

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

18           (2) Use information, including a persistent unique identifier, that is  
19           created or gathered by the operator’s site, service, or application to amass a  
20           profile about a student, except in furtherance of PreK–12 school purposes.

21           “Amass a profile” does not include the collection and retention of account

1 information that remains under the control of the student, the student’s parent  
2 or legal guardian, or the school.

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

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

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

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

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

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

21 (C) to respond to judicial process;

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

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

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

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

15           § 2443b. OPERATOR DUTIES

16           An operator shall:

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

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

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

9           § 2443c. PERMISSIVE USE OR DISCLOSURE

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

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

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



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

4           § 2443d. OPERATOR ACTIONS THAT ARE NOT PROHIBITED

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

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

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

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

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

19                (A) additional content relating to an educational, other learning, or  
20                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; or

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; and

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

10 § 2443e. APPLICABILITY

11 This subchapter does not:

12 (1) limit the authority of a law enforcement agency to obtain any content  
13 or 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  
2           schools or 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 subchapter;

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

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

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

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

19           § 2443f. ENFORCEMENT

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

1       Sec. 5. STUDENT PRIVACY; REVIEW; RECOMMENDATIONS

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

7                               \* \* \* Automatic Renewal Provisions \* \* \*

8       Sec. 6. 9 V.S.A. § 2454a is amended to read:

9       § 2454a. CONSUMER CONTRACTS; AUTOMATIC RENEWAL

10       (a) A contract between a consumer and a seller or a lessor with an initial  
11       term of one year or longer that renews for a subsequent term that is longer than  
12       one month shall not renew automatically unless:

13           (1) the contract states clearly and conspicuously the terms of the  
14       automatic renewal provision in plain, unambiguous language in bold-face type;  
15       and

16           (2) ~~in addition to accepting the contract, the consumer takes an~~  
17       ~~affirmative action to opt in to the automatic renewal provision; and~~

18           (3) ~~if the consumer opts in to the automatic renewal provision, the seller~~  
19       or lessor provides a written or electronic notice to the consumer:

20           (A) not less than 30 days and not more than 60 days before the  
21       earliest of:

- 1 (i) the automatic renewal date;
- 2 (ii) the termination date; or
- 3 (iii) the date by which the consumer must provide notice to cancel
- 4 the contract; and

5 (B) that includes:

- 6 (i) the date the contract will terminate and a clear statement that
- 7 the contract will renew automatically unless the consumer cancels the contract
- 8 on or before the termination date; and
- 9 (ii) the length and any additional terms of the renewal period;
- 10 ~~(iii) one or more methods by which the consumer can cancel the~~
- 11 ~~contract; and~~
- 12 ~~(iv) contact information for the seller or lessor.~~

13 (b) A seller or lessor under a contract subject to subsection (a) of this

14 section shall:

- 15 (1) provide to the consumer a toll-free telephone number, electronic-
- 16 mail address, a postal address if the seller or lessor directly bills the consumer,
- 17 or another cost-effective, timely, and easy-to-use mechanism for canceling the
- 18 contract; and
- 19 (2) if the consumer accepted the contract online, permit the consumer to
- 20 terminate the contract exclusively online, which may include a termination e-

1 mail formatted and provided by the seller or lessor that the consumer can send  
2 without additional information.

3 (c) A person who violates a provision of ~~subsection (a)~~ of this section  
4 commits an unfair and deceptive act in commerce in violation of section 2453  
5 of this title.

6 ~~(e)~~(d) The provisions of this section do not apply to:

7 (1) a contract between a consumer and a financial institution, as defined  
8 in 8 V.S.A. § 11101, or between a consumer and a credit union, as defined in  
9 8 V.S.A. § 30101; or

10 (2) a contract for insurance, as defined in 8 V.S.A. § 3301a.

11 \* \* \* Effective Date \* \* \*

12 Sec. 7. EFFECTIVE DATE

13 (a) This section and Secs. 1–5 of this act shall take effect on July 1, 2019.

14 (b) Sec. 6 of this act shall take effect on July 1, 2019 and supersedes  
15 contrary provisions of 2018 Acts and Resolves No. 179, Sec. 1.

1  
2  
3  
4  
5  
6  
7  
8  
9

(Committee vote: \_\_\_\_\_)

\_\_\_\_\_

Representative \_\_\_\_\_

FOR THE COMMITTEE