

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 non-state entities,
14 including municipalities;

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

1 (9) “Login credentials” means a consumer’s user name or email address,
2 in combination with a password or an answer to a security question, that
3 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, or a consumer’s Social Security
6 number, in combination with any one or more of the following digital data
7 elements, when ~~either the name~~ if the Social Security number or the data
8 elements are not encrypted, or redacted, or protected by another method that
9 renders them unreadable or unusable by unauthorized persons:

10 (i) a Social Security number;

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

17 (iii) a 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) a ~~account passwords~~ password, or personal identification
21 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) health information about a consumer's medical history,
8 mental condition, or physical condition, or about a health care professional's
9 medical diagnosis or treatment of the consumer; and

10 (viii) user name or email address, in combination with a password
11 or an answer to a security question, that together permit access to an online
12 account.

13 (vii)(I) medical history, medical treatment by a health care
14 professional, or diagnosis of mental or physical condition by a health care
15 professional;

16 (II) health status information that a data collector actively
17 collects or generates through inferences; or

18 (III) a health insurance policy number.

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

1 ~~(10)~~ (11) “Record” means any material on which written, drawn, spoken,
2 visual, or electromagnetic information is recorded or preserved, regardless of
3 physical form or characteristics.

4 ~~(11)~~ (12) “Redaction” means the rendering of data so that the data are
5 unreadable or are truncated so that no more than the last four digits of the
6 identification number are accessible as part of the data.

7 ~~(12)~~ (13) (A) “Security breach” means unauthorized acquisition of,
8 electronic data or a reasonable belief of an unauthorized acquisition of,
9 electronic data that compromises the security, confidentiality, or integrity of a
10 consumer’s personally identifiable information or login credentials maintained
11 by a data collector.

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

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

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

4 (ii) indications that the information has been downloaded or
5 copied;

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

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

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

11 § 2435. NOTICE OF SECURITY BREACHES

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

13 (b) Notice of breach.

14 (1) Except as ~~set forth~~ otherwise provided in subsection (d) of this
15 section, any data collector that owns or licenses computerized personally
16 identifiable information **or login credentials** ~~that includes personal information~~
17 ~~concerning a consumer~~ shall notify the consumer that there has been a security
18 breach following discovery or notification to the data collector of the breach.
19 Notice of the security breach shall be made in the most expedient time possible
20 and without unreasonable delay, but not later than 45 days after the discovery
21 or notification, consistent with the legitimate needs of the law enforcement

1 agency, as provided in subdivisions (3) and (4) of this subsection (b), or with
2 any measures necessary to determine the scope of the security breach and
3 restore the reasonable integrity, security, and confidentiality of the data system.

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

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

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

20 (B)(i) The data collector shall notify the Attorney General or the
21 Department, as applicable, of the date of the security breach and the date of

1 discovery of the breach and shall provide a preliminary description of the
2 breach within 14 business days, consistent with the legitimate needs of the law
3 enforcement agency as provided in this subdivision (3) and subdivision (4) of
4 this subsection (b), of the data collector's discovery of the security breach or
5 when the data collector provides notice to consumers pursuant to this section,
6 whichever is sooner.

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

16 (iii) If the date of the breach is unknown at the time notice is sent
17 to the Attorney General or to the Department, the data collector shall send the
18 Attorney General or the Department the date of the breach as soon as it is
19 known.

20 (iv) Unless otherwise ordered by a court of this State for good
21 cause shown, a notice provided under this subdivision (3)(B) shall not be

1 disclosed to any person other than the Department, the authorized agent or
2 representative of the Attorney General, a State’s Attorney, or another law
3 enforcement officer engaged in legitimate law enforcement activities without
4 the consent of the data collector.

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

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

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

20 (4)(A) The notice to a consumer required by this subsection shall be
21 delayed upon request of a law enforcement agency. A law enforcement agency

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

16 (B) A Vermont law enforcement agency with a reasonable belief that
17 a security breach has or may have occurred at a specific business shall notify
18 the business in writing of its belief. The agency shall also notify the business
19 that additional information on the security breach may need to be furnished to
20 the Office of the Attorney General or the Department of Financial Regulation
21 and shall include the website and telephone number for the Office and the

1 Department in the notice required by this subdivision. Nothing in this
2 subdivision shall alter the responsibilities of a data collector under this section
3 or provide a cause of action against a law enforcement agency that fails,
4 without bad faith, to provide the notice required by this subdivision.

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

9 (A) the incident in general terms;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 ~~(HH)~~ 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 (c) In the event a data collector provides notice to more than 1,000
8 consumers at one time pursuant to this section, the data collector shall notify,
9 without unreasonable delay, all consumer reporting agencies that compile and
10 maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. §
11 1681a(p), of the timing, distribution, and content of the notice. This subsection
12 shall not apply to a person who is licensed or registered under Title 8 by the
13 Department of Financial Regulation.

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

1 reasonably possible, the data collector shall provide notice of its determination
2 that misuse of the ~~personal information~~ personally identifiable information or
3 login credentials is not reasonably possible and a detailed explanation for said
4 determination to the Vermont Attorney General or to the Department of
5 Financial Regulation in the event that the data collector is a person or entity
6 licensed or registered with the Department under Title 8 or this title. The data
7 collector may designate its notice and detailed explanation to the Vermont
8 Attorney General or the Department of Financial Regulation as “trade secret”
9 if the notice and detailed explanation meet the definition of trade secret
10 contained in 1 V.S.A. § 317(c)(9).

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

18 (3) If a security breach is limited to an unauthorized acquisition of
19 personally identifiable information comprising a consumer’s name or Social
20 Security number and login credentials, as specified in subdivision
21 2430(9)(A)(viii) of this title, for an online account other than an email account:

1 ~~(A) the data collector shall provide notice of the security breach~~
2 ~~to the consumer electronically and shall advise the consumer to take steps~~
3 ~~necessary to protect the online account, including to change his or her login~~
4 ~~credentials for the account and for any other account for which the consumer~~
5 ~~uses the same login credentials; and~~

6 ~~(B) if the personally identifiable information was login credentials~~
7 ~~were acquired directly from the data collector or its agent, the data collector~~
8 ~~shall provide notice of the security breach to the Attorney General or~~
9 ~~Department of Financial Regulation, as applicable.~~

10 ~~(4) If a security breach is limited to an unauthorized acquisition of~~
11 ~~personally identifiable information comprising a consumer's name or Social~~
12 ~~Security number and login credentials, as specified in subdivision~~
13 ~~2430(9)(A)(viii) of this title, for an email account:~~

14 ~~(A) the data collector shall not provide notice of the security breach~~
15 ~~through the email account; and~~

16 ~~(B) the data collector shall provide notice of the security breach,~~
17 ~~including by clear and conspicuous notice delivered to the consumer online~~
18 ~~when the consumer is connected to the online account from an Internet~~
19 ~~protocol address or online location from which the data collector knows the~~
20 ~~consumer customarily accesses the account.~~

1 (e) Any person subject to this chapter and to the Health Insurance
2 Portability and Accountability Act of 1996 (P.L. 104-191, as amended)
3 (HIPAA) which maintains procedures for Security Breach notification
4 pursuant to HIPAA is deemed to be in compliance with this chapter as it
5 pertains to security breaches involving PII that only includes Protected Health
6 Information (as defined by HIPAA) or health insurance policy numbers, if the
7 person notifies affected Vermont residents in accordance with the maintained
8 procedures when a breach of security occurs.

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

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

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

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

20 (⊕) (g) Except as provided in subdivision (3) of this subsection (f), a
21 financial institution that is subject to the following guidances, and any

1 revisions, additions, or substitutions relating to an interagency guidance shall
2 be exempt from this section:

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

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

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

16 ~~(g)~~ (h) Enforcement.

17 (1) With respect to all data collectors and other entities subject to this
18 subchapter, other than a person or entity licensed or registered with the
19 Department of Financial Regulation under Title 8 or this title, the Attorney
20 General and State's Attorney shall have sole and full authority to investigate
21 potential violations of this subchapter and to enforce, prosecute, obtain, and

1 impose remedies for a violation of this subchapter or any rules or regulations
2 made pursuant to this chapter as the Attorney General and State’s Attorney
3 have under chapter 63 of this title. The Attorney General may refer the matter
4 to the State’s Attorney in an appropriate case. The Superior Courts shall have
5 jurisdiction over any enforcement matter brought by the Attorney General or a
6 State’s Attorney under this subsection.

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

14 * * * Student Data Privacy * * *

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

16 Subchapter 3A: Student Privacy

17 § 2443. DEFINITIONS

18 As used in this subchapter:

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

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

2 (ii) made publicly available pursuant to the federal Family

3 Educational and Rights and Privacy Act; and

4 (B)(i) created by or provided to an operator by a student or the

5 student’s parent or legal guardian in the course of the student’s, parent’s, or

6 legal guardian’s use of the operator’s site, service, or application for PreK–12

7 school purposes;

8 (ii) created by or provided to an operator by an employee or agent

9 of a school or school district for PreK–12 school purposes; or

10 (iii) gathered by an operator through the operation of its site,

11 service, or application for PreK–12 school purposes and personally identifies a

12 student, including information in the student’s education record or electronic

13 mail; first and last name; home address; telephone number; electronic mail

14 address or other information that allows physical or online contact; discipline

15 records; test results; special education data; juvenile dependency records;

16 grades; evaluations; criminal records; medical records; health records; social

17 security number; biometric information; disability status; socioeconomic

18 information; food purchases; political affiliations; religious information; text

19 messages; documents; student identifiers; search activity; photos; voice

20 recordings; or geolocation information.

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

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

12 (4) “School” means:

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

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

19 (5) “Targeted advertising” means presenting advertisements to a student
20 where the advertisement is selected based on information obtained or inferred
21 over time from that student’s online behavior, usage of applications, or covered

1 information. The term does not include advertising to a student at an online
2 location based upon that student’s current visit to that location or in response to
3 that student’s request for information or feedback, without the retention of that
4 student’s online activities or requests over time for the purpose in whole or in
5 part of targeting subsequent ads.

6 § 2443a. OPERATOR PROHIBITIONS

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

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

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

18 “Amass a profile” does not include the collection and retention of account
19 information that remains under the control of the student, the student’s parent
20 or legal guardian, or the school.

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

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

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

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

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

17 (B) to ensure legal and regulatory compliance or take precautions
18 against liability;

19 (C) to respond to judicial process;

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

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

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

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

13 § 2443b. OPERATOR DUTIES

14 An operator shall:

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

19 (2) delete, within a reasonable time period and to the extent practicable,
20 a student’s covered information if the school or school district requests
21 deletion of covered information under the control of the school or school

1 district, unless a student or his or her parent or legal guardian consents to the
2 maintenance of the covered information; and

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

6 § 2443c. PERMISSIVE USE OR DISCLOSURE

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

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

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

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

1 § 2443d. OPERATOR ACTIONS THAT ARE NOT PROHIBITED

2 This subchapter does not prohibit an operator from doing any of the
3 following:

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

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

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

14 (4) using recommendation engines to recommend to a student either of
15 the following:

16 (A) additional content relating to an educational, other learning, or
17 employment opportunity purpose within an online site, service, or application
18 if the recommendation is not determined in whole or in part by payment or
19 other consideration from a third party; or

20 (B) additional services 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; and

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

6 § 2443e. APPLICABILITY

7 This subchapter does not:

8 (1) limit the authority of a law enforcement agency to obtain any content
9 or information from an operator as authorized by law or under a court order;

10 (2) limit the ability of an operator to use student data, including covered
11 information, for adaptive learning or customized student learning purposes;

12 (3) apply to general audience Internet websites, general audience online
13 services, general audience online applications, or general audience mobile
14 applications, even if login credentials created for an operator’s site, service, or
15 application may be used to access those general audience sites, services, or
16 applications;

17 (4) limit service providers from providing Internet connectivity to
18 schools or students and their families;

19 (5) prohibit an operator of an Internet website, online service, online
20 application, or mobile application from marketing educational products
21 directly to parents if the marketing did not result from the use of covered

1 information obtained by the operator through the provision of services covered
2 under this subchapter;

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

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

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

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

14 § 2443f. ENFORCEMENT

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

17 Sec. 5. STUDENT PRIVACY; REVIEW; RECOMMENDATIONS

18 The Attorney General, in consultation with the Agency of Education, shall
19 examine the issue of student data privacy as it relates to the federal Family
20 Educational Rights and Privacy Act and access to student data by data brokers

1 or other entities, and shall confer with parties of interest to determine any
2 necessary recommendations.

3 * * * Effective Date * * *

4 Sec. 6. EFFECTIVE DATE

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

6

7

8

9

10 (Committee vote: _____)

11

12

Representative _____

13

FOR THE COMMITTEE