SENATE
STATE OF MINNESOTA
EIGHTY-NINTH SESSION

S.F. No. 2845

(SENATE AUTHORS: NIENOW and Dibble)

DATE	D-PG	OFFICIAL STATUS
03/17/2016	5103	Introduction and first reading Referred to Education

A bill for an act

relating to data privacy; protecting student privacy in data on electronic devices provided by an educational institution; providing penalties; proposing coding for new law in Minnesota Statutes, chapter 125B.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. **[125B.30] DEFINITIONS.**

(a) For the purposes of sections 125B.30 to 125B.34, the following terms have the meanings given them.

(b) "1-to-1 program" means any program authorized by an educational institution where a technological device is provided to a student by or through an educational institution for overnight or at-home use.

(c) "1-to-1 device" means a technological device provided to a student pursuant to a 1-to-1 program.

(d) "1-to-1 device provider" means a person or entity that provides a 1-to-1 device to a student or educational institution pursuant to a 1-to-1 program, and includes any business or nonprofit entities that share a parent, subsidiary, or sister relationship with the entity that provides the 1-to-1 device.

(e) "Aggregate data" means student-related data collected and reported by an educational institution at the group, cohort, or institutional level that contains no personally identifiable student information.

(f) "De-identified" means having removed or obscured any personally identifiable information from personally identifiable student information in a manner that prevents the unintended disclosure of the identity of the student or information about the student.

Information shall not be considered de-identified if it meets the definition of "personally identifiable student information" in paragraph (n).

(g) "Educational institution" means:

(1) a private or public school, institution, or school district, or any subdivision thereof, that offers participants, students, or trainees an organized course of study or training that is academic, trade-oriented, or preparatory for gainful employment, as well as school employees acting under the authority or on behalf of an educational institution; or

(2) a state or local educational agency authorized to direct or control an entity in clause (1).

(h) "Educational record" means an educational record as defined by United States Code, title 20, section 1232g(a)(4), on the effective date of this section.

(i) "Education research" means the systematic gathering of empirical information to advance knowledge, answer questions, identify trends, or improve outcomes within the field of education.

(j) "Elementary school" means the grade levels falling under the definition of "elementary school," as that term is interpreted by state law for purposes of section 9101 of the Elementary and Secondary Education Act of 1965 (United States Code, title 20, section 7801 et seq.).

(k) "Law enforcement official" means an officer or employee of any agency or authority of the state of Minnesota, or a political subdivision or agent thereof, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law, make arrests, or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

(l) "Location tracking technology" means any hardware, software, or application that collects or reports data that identifies the geophysical location of a technological device.

(m) "Opt-in agreement" means a discrete, verifiable, written, or electronically generated agreement by which, subject to the provisions of sections 125B.30 to 125B.34, a student or the student's parent or legal guardian voluntarily grants a school employee, SIS provider, or 1-to-1 device provider with limited permission to access and interact with a specifically defined set of personally identifiable student information.

(n) "Personally identifiable student information" means one or more of the following:

(1) a student's name;

(2) the name of a student's parent, legal guardian, or other family member;

(3) the address of a student or student's parent, legal guardian, or other family member;

(4) a photograph, video, or audio recording that contains the student's image or voice;

(5) indirect identifiers, including but not limited to a student's date of birth, place of birth, mother's maiden name, Social Security number, student number, biometric record, telephone number, credit card account number, insurance account number, financial services account number, customer number, persistent online identifier, e-mail address, social media address, or other electronic address;

(6) any aggregate or de-identified student data that is capable of being disaggregated or reconstructed to the point that individual students can be identified; and

(7) any student data or other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person who does not have personal knowledge of the relevant circumstances to identify a specific student with reasonable certainty.

(o) "School employee" means an individual who is employed by an educational institution, compensated through an annual salary or hourly wage paid by an educational institution, and whose services are primarily rendered at a physical location that is owned or leased by that educational institution. For purposes of sections 125B.30 to 125B.34, individuals with law enforcement or school security responsibilities, including school resource officers, school district police officers, contract or private security companies, security guards, or other law enforcement personnel are not school employees.

(p) "Student" means any student, participant, or trainee, whether full time or part time, in an organized course of study at an educational institution.

(q) "Student data" means data that is collected and stored by an educational institution, or by a person or entity acting on behalf of that institution, and included in a student's educational record.

(r) "Technological device" means any computer, cellular phone, smartphone, digital camera, video camera, audio recording device, or other electronic device that can be used for creating, storing, or transmitting information in the form of electronic data.

Sec. 2. **[125B.31] 1-TO-1 PROGRAMS.**

Subdivision 1. **General rule.** When an educational institution or 1-to-1 device provider provides a student with a technological device pursuant to a 1-to-1 program, no school employee or 1-to-1 device provider, or an agent thereof, may access or track such a device or the activity or data thereupon, either remotely or in person, except in accordance with the provisions of this section.

Subd. 2. **Exceptions.** No school employee or 1-to-1 device provider, or an agent thereof, may access any data input into, stored upon, or sent or received by a student's

1-to-1 device, including but not limited to its browser, keystroke, or location history, nor may such data be analyzed, interacted with, shared, or transferred unless:

(1) the data being collected is not personally identifiable student information;

(2) the data is being accessed by or on behalf of a school employee who:

(i) is the student's teacher;

(ii) is receiving or reviewing the information for an educational purpose consistent with the teacher's professional duties; and

(iii) does not use the information, or permit any other person or entity to use the information, for any other purpose;

(3) a school employee or 1-to-1 device provider or an agent thereof has been authorized to access specific personally identifiable student information pursuant to an opt-in agreement under subdivision 9;

(4) a school employee has a reasonable suspicion that the student has violated or is violating an educational institution policy and that data on the 1-to-1 device contains evidence of the suspected violation, subject to the following limitations:

(i) prior to searching a student's 1-to-1 device based on reasonable individualized suspicion, the school employee shall document the reasonable individualized suspicion and notify the student and the student's parent or legal guardian of the suspected violation and what data will be accessed in searching for evidence of the violation. An educational institution, subject to any other relevant legal restrictions, may seize a student's 1-to-1 device to prevent data deletion pending notification, provided that:

(A) the prenotification seizure period is no greater than 48 hours; and

(B) the 1-to-1 device is stored securely on educational institution property and not accessed during the prenotification seizure period;

(ii) searches of a student's device based upon a reasonable individualized suspicion that an educational institution policy has been violated shall be strictly limited to finding evidence of the suspected policy violation and shall immediately cease upon finding sufficient evidence of the suspected violation. It shall be a violation of this item to copy, share, or transfer any data, or any information thereabout, that is unrelated to the specific suspected violation which prompted the search of the 1-to-1 device; and

(iii) when a student is suspected of illegal conduct, no search of the 1-to-1 device may occur unless a judicial warrant has been secured according to clause (5) even if the student is also suspected of a related or unrelated violation of educational institution policy;

(5) a school employee or law enforcement official reasonably suspects the student has engaged or is engaging in illegal conduct, reasonably suspects data on the 1-to-1

device contains evidence of the suspected illegal conduct, and has secured a judicial warrant for a search of the device;

(6) doing so is necessary to update or upgrade a device's software, or protect the device from cyberthreats, and access is limited to that purpose;

(7) doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose. Within 72 hours of accessing a 1-to-1 device's data in response to an imminent threat to life or safety, the school employee or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution with a written description of the precise threat that prompted the access and what data was accessed; or

(8) the information sent from the device is posted on a Web site that:

(i) is accessible by the general public; or

(ii) is accessible by a specific school employee who was granted permission by the student to view the content.

Subd. 3. **Use of location tracking technology.** No school employee or 1-to-1 device provider, or an agent thereof, may use a student's 1-to-1 device's location tracking technology to track a device's real-time or historical location, unless:

(1) such use is ordered pursuant to a judicial warrant;

(2) the student to whom the device was provided, or the student's parent or legal guardian, has notified a school employee or law enforcement official that the device is missing or stolen; or

(3) doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose. Within 72 hours of accessing a 1-to-1 device's location tracking technology in response to an imminent threat to life or safety, the school employee or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the precise threat that prompted the access and what data and features were accessed.

Subd. 4. **No access to audio or video receiving, transmitting, or recording functions; exceptions.** No school employee or 1-to-1 device provider, or an agent thereof, may activate or access any audio or video receiving, transmitting, or recording functions on a student's 1-to-1 device, unless:

(1) a student initiates a video chat or audio chat with the school employee or 1-to-1 device provider;

(2) the activation or access is ordered pursuant to a judicial warrant; or

(3) doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose. Within 72 hours of accessing a 1-to-1 device's audio or video receiving, transmitting, or recording functions in response to an imminent threat to life or safety, the school employee or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the precise threat that prompted the access and what data and features were accessed.

Subd. 5. **No access to student's password-protected software, Web site accounts, or applications; exceptions.** No school employee, or an agent thereof, may use a 1-to-1 device, or require a student to use a 1-to-1 device in their presence, in order to view or gain access to a student's password-protected software, Web site accounts or applications, except where:

(1) the school employee is a teacher;

(2) the student is enrolled in and participating in a class taught by the teacher; and

(3) the viewing of the 1-to-1 device relates exclusively to an educational purpose.

Subd. 6. **Prohibited uses of student data.** No 1-to-1 device provider, or an agent thereof, may use any student data or personally identifiable student information stored on or retrieved from a 1-to-1 device to:

(1) inform, influence, or direct marketing or advertising efforts directed at a student, a student's parent or legal guardian, or a school employee, except pursuant to a valid opt-in agreement; or

(2) develop, in full or in part, a student profile for any commercial or other noneducational purpose.

Subd. 7. **Training required.** Notwithstanding any other provisions in this section, no school employee may supervise, direct, or participate in a 1-to-1 program, or access any 1-to-1 device or data thereupon, until the school employee has received adequate training to ensure the school employee's understanding and compliance with the provisions of this section.

Subd. 8. **No sharing of personally identifiable student information; exceptions.** No personally identifiable student information obtained or received from a 1-to-1 device by a school employee or 1-to-1 device provider may be sold, shared, or otherwise transferred to another person or entity, except:

(1) to another school employee who has satisfied the requirements of subdivision 7 and is accessing the information in furtherance of the employee's professional duties; or

(2) where a 1-to-1 device provider has been authorized to do so pursuant to an opt-in agreement under subdivision 9.

Subd. 9. **Opt-in agreements.** (a) For purposes of this section, a valid opt-in agreement shall identify, with specificity:

(1) the precise subset of personally identifiable student information on the 1-to-1 device to which the authority to access, analyze, and interact is being granted;

(2) the name of the school employee or 1-to-1 device provider to whom the authority to access, analyze, and interact with the personally identifiable student information on the 1-to-1 device is being granted;

(3) the educational purpose for which the school employee or 1-to-1 device provider is being granted the authority to access, analyze, and interact with the personally identifiable student information on the 1-to-1 device; and

(4) the individual student to whom the opt-in agreement applies.

(b) An opt-in agreement shall only be valid if it has been signed by:

(1) the student's parent or guardian, if the student is in elementary school;

(2) the student and the student's parent or legal guardian, if the student has advanced beyond elementary school but has not yet reached the age of majority; or

(3) the student alone, if the student has reached the age of majority.

(c) An opt-in agreement shall not be valid if it actually or effectively grants a 1-to-1 device provider:

(1) general authority to access a student's 1-to-1 device; or

(2) the authority to collect all the personally identifiable student information that is generated by or used in connection with a specific program or application.

(d) An opt-in agreement may be revoked at any time, upon written notice to an educational institution, by the person eligible to authorize an opt-in agreement pursuant to paragraph (b). Within 30 days of such a revocation, notice to any affected third parties shall be made by the educational institution.

(e) A 1-to-1 device provider that accesses, analyzes, or interacts with personally identifiable student information on a 1-to-1 device shall bear the burden of proving that it acted pursuant to a valid opt-in agreement.

(f) No 1-to-1 device program offered to an educational institution or its students may be conditioned upon the exclusive use of any software, application, Web site, or Internet-based service sold to or provided by the 1-to-1 device provider.

(g) No 1-to-1 device or related educational benefit may be withheld from, or punitive measure taken against, a student or the student's parent or legal guardian:

(1) based in whole or in part upon a decision not to sign, or to revoke, an opt-in agreement; or

(2) based in whole or in part upon a student's refusal to open, close, or maintain an e-mail or other electronic communications or social media account with a specific service provider.

(h) A 1-to-1 device provider shall violate paragraph (g), clause (1), if it conditions the offer, provision, or receipt of a 1-to-1 device upon a student's or the student's parent's or legal guardian's agreement to provide access to personally identifiable student information.

Subd. 10. **No sale, sharing, or transfer of personally identifiable student information; exception.** No school employee or 1-to-1 device provider, or an agent thereof, who receives or collects personally identifiable student information from a 1-to-1 device may share, sell or otherwise transfer such data to another person or entity unless, in the case of a 1-to-1 device provider, such information is sold as part of a sale or merger of the entirety of the 1-to-1 device provider's business. Any entity that purchases personally identifiable student information pursuant to subdivision 9, paragraph (c), shall be subject to the same restrictions and obligations under this section as the 1-to-1 device provider from which the personally identifiable student information was obtained.

Subd. 11. **Direct access prohibited; exceptions.** No person or entity, other than an educational institution, school employee, or 1-to-1 device provider subject to the limitations set forth in this section, shall be provided direct access to review or interact with a 1-to-1 device and the data thereon, unless otherwise authorized to do so by law, pursuant to a judicial warrant, or upon the express permission of the student to whom the 1-to-1 device is issued.

Subd. 12. **Return of 1-to-1 device; erase data.** When a 1-to-1 device is permanently returned by a student, the educational institution or 1-to-1 device provider who provided it shall, without otherwise accessing the data on the 1-to-1 device, fully erase all the data stored on the device and return the device to its default factory settings.

Subd. 13. **Personally identifiable student data; general exceptions.** The provisions of section 125B.32 that relate to the collection and use of personally identifiable student information shall not apply to personally identifiable student information collected by a 1-to-1 provider from a software program, Web site or application that was:

(1) not preloaded on the 1-to-1 device;

(2) not the target of a link that was preloaded on the 1-to-1 device; and

(3) not promoted, marketed, or advertised in connection with the issuance of the 1-to-1 device.

Sec. 3. **[125B.32] LIMITATIONS ON USE.**

Evidence or information obtained or collected in violation of sections 125B.30 to 125B.34 shall not be admissible in any civil or criminal trial or legal proceeding, disciplinary action, or administrative hearing.

Sec. 4. **[125B.33] PENALTIES.**

(a) Any person or entity who violates sections 125B.30 to 125B.34 shall be subject to legal action for damages or equitable relief, to be brought by any other person claiming that a violation of sections 125B.30 to 125B.34 has injured that person or that person's reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured on account of violation of the provisions of sections 125B.30 to 125B.34, and reasonable attorney fees and other costs of litigation.

(b) Any school employee who violates sections 125B.30 to 125B.34, or any implementing rule or regulation, may be subject to disciplinary proceedings and punishment. For school employees who are represented under the terms of a collective bargaining agreement, sections 125B.30 to 125B.34 prevail except where they conflict with the collective bargaining agreement, any memorandum of agreement or understanding signed pursuant to the collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit.

Sec. 5. **[125B.34] SEVERABILITY.**

The provisions in sections 125B.30 to 125B.34 are severable. If any part or provision of sections 125B.30 to 125B.34, or the application of sections 125B.30 to 125B.34 to any person, entity, or circumstance, is held invalid, the remainder of sections 125B.30 to 125B.34, including the application of such part or provision to other persons, entities, or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Sec. 6. **EFFECTIVE DATE.**

Sections 1 to 5 are effective January 1, 2017.