HOUSE RESEARCH

Bill Summary

File Number: H.F. 1507 **Date:** April 4, 2017
Version: As introduced

Authors: Lucero

Subject: The Student Data Privacy Act

Analyst: Cristina Parra
Mary Mullen

Overview

This bill creates a Student Data Privacy Act. The Act specifically regulates how data on computer devices that students are issued by the school and allowed to take home can be accessed, as well as the student's data that is stored and transmitted by software programs on those devices.

This Act provides restrictions on how student data can be used, accessed, sold, shared, or kept specifically related to the retention or transmission of data on one-to-one computer devices and the software programs which are used by the student or school to maintain educational information and data. The Act supplements the existing student data provisions in the Minnesota Data Practices Act and the federal Family Educational Rights and Privacy Act (FERPA) to provide the parameters of access for teachers and schools to student information on certain software apps and computer devices which students use to complete homework and do other work required for their K-12 education. The Act applies to all schools and the hardware and software providers they contract with, but do not apply to homeschools.

The law also requires training on student data privacy, allows for civil cause of action for violations of the act, and clarifies the admissibility of evidence obtained in violation of the Student Data Privacy Act in criminal and civil cases.

Section

1 **Technology devices for students.** Adds a cross-reference to the Minnesota Data Practices Act indicating that the Student Data Privacy Act in 125B.30 to 125B.36 contains provisions regarding access and use of student data.

2 **Citation.** Provides that the new sections of law created by this bill can be cited as the Student Data Privacy Act.

3 **Definitions.** Provides the definitions for the Student Data Privacy Act, including:

- "Aggregate data" is data on a group of students that does not have personally identifiable student information.
- "De-identified data" is data that removes or obscures information to protect a student's identity.
- "Educational data" means any data on or about a student except for law enforcement data or personnel data which is excluded by section 13.32.
- "Educational research" is research done using student data by an educational institution.
- "Educational institutions" include public schools, nonpublic schools, charter schools, and the state and local educational agencies that control schools. "Educational institutions" does not include a home school.
- "Location tracking technology" means hardware such as a computer, tablet, or phone and software such as a computer program or app that collects or reports data to provide the location of that electronic device.
- "One-to-one device" is the technological device (such as a computer or tablet) that the school provides to a student for use at home or away from the school.
- "One-to-one device provider" means the nonprofit or business that provides the computers or tablets to the school for use by the students at home or outside the school.
- "One-to-one program" means the program where the school provides a technological device (such as a computer or tablet) to a student for overnight use or use at home or outside the school.
- "Opt-in-agreement" this is the written or electronic agreement which is signed by a parent, guardian, or student that allows the school, software provider, or the company providing the electronic devices to access the educational data for that student.
- "Personally identifiable student information" means data maintained by a school or educational agency on a student when the data appears with: the student's name; the name of the student's parent or other family members; the student's address; Social Security number; student identification number; biometric records; date of birth; or other data that would allow the student to be identified.
- "SIS" means a student information system which is a software application or cloud-based service that allows a school to input or maintain data on students, including tracking or sharing student data in real time.

Section

- "SIS provider" is a business or nonprofit that provides or maintains the software or app on the computers or tablets used by the schools which can access, collect, or track student data.
- "Technology device" includes computers, phones, cameras, recording devices, and any electronic device used to create, store, or transmit electronic data.

4 Student information systems.

Subd. 1. SIS contracts; requirements; prohibitions. Provides specific requirements that must be in a contract between a school and a software provider related to the security of the student data transmitted or collected, and requires that the contracts include provisions identifying: who owns the data, how to handle a data breach, how and when data must be destroyed, how and when data can be accessed, and prohibitions on the sale of data. This subdivision provides that when the contract is with a public educational institution the contract must include language that adds the Minnesota Data Practices Act requirements to the contracting SIS.

Subd. 2. Opt-in agreements. Provides the necessary information that must be provided in the agreement between the parent (or student if they are over 18) and the school or software provider related to the sharing of data. This subdivision also extends the restrictions on use of the data to other persons possessing the data and prohibits the transfer, sale, or use of the data except as otherwise allowed in Student Data Privacy Act. This subdivision allows a parent or student to revoke access to data, requires a parent or student to sign a new agreement each year, and prohibits the school or educational agency from penalizing a student for refusing to sign or for revoking an opt-in agreement.

Subd. 3. School employees. Allows school employees to access student data to perform their professional duties and provides specific requirements about when a teacher or other school employee can transfer or share student data and when the data must be destroyed.

Subd. 4. Parent or guardian access to student data. Clarifies when students and parents can access data and which data they can access.

Subd. 5. Requirements for deleting data in an SIS. Requires a school to delete all student information and data on the software or app within one year after a student graduates, withdraws, or is expelled from a school, but does not include the student's Social Security number, transcript, graduation record, letters of recommendations or other information required by postsecondary institutions for admission to the institution, or data used in past or ongoing disciplinary proceedings, de-identified data, or student data required by a court order or warrant to be maintained.

Subd. 6. Requirements for deleting physical or digital copies of student data. Requires a software provider or another third party accessing student data to destroy all physical or digital copies of the data within 180 days of receiving notice that a student has graduated, been expelled, or withdrawn. This requirement does not apply to information related to a disciplinary action or court case, aggregate or de-identified

Section

data, data required to be maintained by law or court order, and where the student or parent and the school and software provider have all agreed to maintain the data.

Subd. 7. Notice to SIS provider and third parties. Requires a school to notify a software provider when a student graduates, withdraws, or is expelled and also requires the software provider to notify any third party who is allowed to access that student's records of the student's changed status.

Subd. 8. Access under law, judicial warrant, or audit. Prohibits a person other than a school, educational agency, school employee, or the software company from accessing the software or the data on the software unless they are authorized by law, authorized through a legally issued warrant, or as part of a school audit.

Subd. 9. Directory information permitted. Allows a vendor providing graduation and class memorabilia products to students to access directory information for students so long as it is used only for that purpose, not sold to another entity, and destroyed after it is used.

Subd. 10. Interaction with other law. Clarifies that other laws that provide greater privacy protections to student's records are not superseded or limited by this section and provides that this section does not change any classifications of student data under the Minnesota Data Practices Act.

5 One-to-one programs; access to data.

Subd. 1. General rule; contracts. Prohibits access to a student's computers or tablets (when they are provided by the school) by the hardware provider or the school or school employees except as allowed by this section of law. Requires certain information to be contained in the contract with device providers, including the extension of the Data Practices Act to the device provider when contracting with a public educational institution.

Subd. 2. Exceptions. Prohibits access and sharing of the student's data, including browser history or location history, except:

(1) by the student's teacher who is reviewing the data for educational purposes in the course of their professional duties, and does not allow anyone else to use or view the data;

(2) when the data is aggregate data or de-identified data;

(3) a school employee or device provider who is authorized to access information via an opt-in agreement;

(4) a school employee who believes the student violated a law or school rule and there is evidence on the device, but only when the school and employee follows specific provisions in this section about how to search the device;

(5) there is a warrant to search the device;

(6) to upgrade the device or software;

Section

(7) access is required to respond to an imminent threat to life or safety and access is limited to the purpose of addressing that threat; or

(8) the information is also posted on a public website or accessible by a school employee through written permission from the student or parent.

Subd. 3. Use of location tracking technology. The school, school employees, device providers, and law enforcement may not track a student's location (in real-time or the saved location information) unless:

- the school or law enforcement has been allowed to access location information by a warrant;
- the student or parent notifies the school or police that the device was stolen; or
- the school or law enforcement need to access the location information to respond to an imminent threat to life or safety.

Subd. 4. No access to audio or video receiving, transmitting, or recording functions; exceptions. Prohibits the school and the device manufacturer or employee from accessing the audio or video on the device (or that is transmitted by the device) unless:

- the student is communicating with ("chatting") with the school employee or device provider;
- a warrant has been issued for the audio or video or transmissions; or
- the school or law enforcement needs to access the device's audio or video functions or the audio or video received or sent from the device to respond to an imminent threat to life or safety.

Subd. 5. No access to student's password-protected software, website accounts, or applications; exceptions. Prohibits a school or employee of a school from looking at a student's websites or software on a computer or other electronic device (one-to-one device) or looking through the device themselves, except that a teacher may require a student in their class to see the one-to-one device as part of their educational program.

Subd. 6. Prohibited uses of student data. Prohibits a device provider or employee from using information about students stored on a device or retrieved from a device to develop a student profile for any commercial purpose or market or advertise to students, parents, or schools except as the opt-in agreement allows.

Subd. 7. Training required. Requires school employees to attend at least annual training in order to access a student's one-to-one device or data from a device, consistent with section 7 of this bill. The training must cover the one-to-one data access allowed under law, as well as the provisions of the Minnesota law on school survey information, and the federal law on student privacy (FERPA).

Subd. 8. No sharing of personally identifiable student information; exceptions. Prevents a school employee or device provider or employee from transferring data they receive that is personally identifiable data on a student to anyone, except:

Section

- they can transfer it to another school employee as part of their professional duties; or
- a device provider can transfer the information consistently with an opt-in agreement signed by the student or parent.

Subd. 9. Opt-in agreement. Requires an opt-in agreement for a device provider to be consistent with the requirements of an opt-in agreement with a software provider in section 4 of this bill and also provides that the other provisions that must be included in an opt-in agreement between a device provider and the parents or student. This section also prohibits certain things from being included in an opt-in agreement, such as allowing general authority to access the device or to collect personal information. This section indicates how an opt-in agreement can be revoked and prevents retaliation for revoking an opt-in agreement, and requires the agreements to be signed annually.

Subd. 10. No sale, sharing, or transfer of personally identifiable student information; exceptions. Prohibits personally identifiable student data from being sold or shared, except when a device provider's business is sold or merged, but then requires the new device provider to be held to all the same restrictions under law related to the student data.

Subd. 11. Direct access prohibited; exceptions. Prohibits access by anyone other than the student, the student's parent or guardian, school, or device provider to the one-to-one devices except as authorized by law, a judicial warrant, or with the express permission of the parent or student.

Subd. 12. Return of one-to-one device; data deletion. Requires the one-to-one computer or tablet to be erased and returned to factory settings within 180 days when the device is permanently returned to the hardware provider or the school. The data contained on the device is not allowed to be accessed by the device provider or the school when it is returned.

Subd. 13. Personally identifiable student data; general exceptions. Provides an exemption for the access to student data on one-to-one devices allowing access to information from software, websites, or other computer apps that were not preloaded onto the device or approved by the school or otherwise advertised or directed to be used with the device.

6 **Limitations on use.** Prohibits the use of information collected or obtained in violation of the provisions of the Student Data Privacy Act in a criminal or civil legal proceeding, student disciplinary action, or administrative hearing.

7 **Annual training required to protect student data.** Requires every school district to conduct annual training for staff, IT directors, teachers and other individuals who access student data on how to comply with FERPA (the federal law on student privacy) to prevent the unauthorized access or disclosure of student data.

8 **Penalties.** Provides a cause of action for monetary damages or equitable relief to a person who is injured due to a violation of the Student Data Privacy Act, including special and general damages, and reasonable attorneys' fees and costs. Provides that the Student Data

Section

Practices Act does not preclude other legal remedies such as the remedies under FERPA and the Minnesota Data Practices Acts when those laws are violated.

9 **Effective date.** Provides that the Student Data Privacy Act is to become effective on January 1, 2018.