HOUSE RESEARCH

Bill Summary

FILE NUMBER: H.F. 2898 **DATE:** March 17, 2016
Version: Delete everything amendment (A16-0882)

Authors: Lucero and others

Subject: Protecting student data under the Minnesota Student Data Privacy Act

Analyst: Lisa Larson

Overview

Proposes student data privacy laws, entitled "The Minnesota Student Data Privacy Act" that, among other things: require parents and adult students to give specific permission to third parties to access student data; limit the ability of schools and third contractors to access information about students made on computing devices loaned to students; protect students' personal technological devices on and off the school campus; and prevent schools from demanding access to students' social media accounts, with some exceptions. Combines the proposals in house files 2898, 2899, and 2900.

Section

1 **Citation.** Allows the sections of this bill to be cited as "The Minnesota Student Data Privacy Act."

2 **Definitions.** (a) Defines terms for purposes of this legislation.

(b) Defines "1-to-1 program" to mean a school program providing a student with a technological device for overnight or at-home use.

(c) Defines "1-to-1 device" to mean a technological device provided to a student participating in a 1-to-1 program.

(d) Defines "1-to-1 device provider" to mean a person or entity providing a 1-to-1 device to a student participating in a 1-to-1 program and includes entities affiliated with the 1-to-1 device provider.

Section

(e) Defines "aggregate data" to mean group, cohort, or institutional student data that contains no personally identifiable student information.

(f) Defines "de-identified data" to mean data from which personally identifiable information is removed or obscured in order to prevent a student's identity or information about that student from being disclosed.

(g) Defines "educational institution" to mean a public or nonpublic K-12 school, excluding a home school, and a public or private postsecondary institution.

(h) Defines "educational record" consistent with the definition of educational record contained in Minnesota Statutes, chapter 13.

(i) Defines "education research" to mean the systematic gathering of empirical information to inform or improve the field of education.

(j) Defines "elementary school" consistent with the definition of elementary school in Minnesota Statutes, chapter 120A.

(k) Defines "law enforcement official" to mean a peace officer or a school resource official under the Minnesota Pupil Fair Dismissal Act.

(l) Defines "location tracking technology" to mean any hardware, software, or application that collects or reports data identifying the location of a technology device.

(m) Defines "opt-in agreement" to mean an agreement by which a parent or adult student grants a school employee or third party contractor or provider with limited access to personally identifiable information about the student.

(n) Defines "personal technological device" to mean a technological device possessed by a student other than a 1-to-1 device.

(o) Defines "personally identifiable student information" to mean the name of a student or a family member of the student, the address of the student or family member, a recording of the student's image or voice, indirect identifiers such as a student's place of birth or Social Security number, among other examples, aggregate or de-identified data that can be disaggregated or reconstructed to identify an individual student, and student data or other information a reasonable person without specific personal knowledge could use to identify an individual student with reasonable certainty.

(p) Defines "school employee" to mean all individuals employed in a school and all individuals who provide services to a school as a volunteer, contractor, or under another agreement.

(q) Defines "SIS provider" to mean an entity that sells, leases, provides, operates, or maintains a student information system for an educational institution.

(r) Defines "student" to mean a person enrolled in a school under Minnesota's compulsory attendance law.

(s) Defines "student data" to mean the data collected and stored by an educational institution or a person or entity acting on its behalf, and included in a student's education record.

Section

(t) Defines "student information system" or "SIS" to mean a software application or cloud-based service that allows an educational institution access to student data, including personally identifiable information, including the ability to track or share personally identifiable student information in real time.

(u) Defines "technological device" to mean any electronic device used to create, store, or transmit information electronically.

3 Student information systems.

Subd. 1. Student information system contracts; requirements; prohibitions. (a) Requires agreements between an educational institution and an SIS provider regarding a student information system to: include appropriate security measures to protect student data, including personally identifiable information; acknowledge no student data belongs to the SIS provider; put in place policies and procedures to respond to data breaches, including various forms of notice to affected parties; require the SIS provider to delete all SIS data and destroy other records containing personally identifiable information within 90 days after terminating the agreement between the educational institution and the SIS provider unless an opt-in agreement allows the SIS provider to retain personally identifiable information on a student for the student's benefit; at the expense of the educational institution, transfer data to another designated SIS provider at the request of the educational institution that is a party to the agreement; and comply with all obligations and restrictions applicable to SIS providers under this act.

(b) Requires agreements under paragraph (a) to prohibit SIS providers from using student data or personally identifiable information input into the SIS unless: an opt-in agreement allows such use; the SIS provider must use the student data to comply with the agreement; the SIS provider responds to a request from the educational institution; the educational institution shares the data for purposes of student health and safety; the SIS provider provides aggregated or delete everything-identified data for purposes of mandated reporting or educational research; or the SIS provider accesses the data for testing and improving SIS value and performance if copied data and data analysis are deleted within 60 days and the data is not sold unless part of a sale or merger of the SIS provider's business. Prohibits using student data for marketing or advertising directed at a student, parent, or school employee unless an opt-in agreement applies or for developing a profile of a student or student group for commercial or other non-educational purposes.

Subd. 2. Opt-in agreements. (a) Requires opt-in agreements to indicate: the student data the SIS provider can access; the name of the SIS provider being granted access to the student data; the educational purposes for which the SIS provider is being granted access; the student to whom the opt-in agreement applies.

(b) Requires the parent of an elementary or secondary student to sign the opt-in agreement and allows an eligible student to sign the agreement otherwise.

(c) Allows a SIS provider to transmit student data only if the transmission is to benefit the educational institution or the student, the personally identifiable information is clearly identified in the agreement, the person receiving the information is clearly

Section

identified in the agreement, the benefit to the educational institution or student is clearly identified, and a record of what is transmitted and with whom is attached to the student's record.

(d) Subjects people and entities accessing student data under subdivision 1 to the same restrictions and obligations that apply to the SIS provider providing the data to the person or entity.

(e) Invalidates an opt-in agreement that grants general access to student data in a SIS system.

(f) Prohibits SIS providers, school employees, and others who receive personally identifiable student information from a SIS under an opt-in agreement from transmitting that information.

(g) Allows the party granting access in an opt-in agreement to revoke the agreement at any time and requires the educational institution to notify the SIS provider within 30 days.

(h) Places on the SIS provider the burden of proving it acted under a valid opt-in agreement.

(i) Prohibits educational institutions from imposing consequences on a parent or eligible student who does not sign or revokes an opt-in agreement.

Subd. 3. School employees. (a) Grants adequately trained school employees access to personally identifiable student data for purposes of carrying out their professional duties.

(b) Prohibits school employees from transmitting personally identifiable student data except where specifically authorized, with the employee's employer, with another school employee who has access to the student data, or where the school employee is a teacher transferring student data for classroom record-keeping or management, third parties with access to the SIS are prohibited from accessing the transmitted data, and the data is deleted within 45 days after it is finally used.

Subd. 4. Parent or guardian access to student data. (a) Allows parents to inspect student data stored on a SIS and to seek to correct or remove inaccurate data in a student's record.

(b) Declares that a parent's right to review a student's record does not apply where the student supplied the information to the educational institution and disclosing the information may threaten the student's health or safety.

(c) Declares that a parent's right to review a student's record does not apply if a parent or student waives access to particular information.

(d) Transfers a parent's right to access a student's record to the adult student.

(e) Requires educational institutions to establish procedures to review records and correct or remove inaccurate data in the record and provide a fair hearing when the institution refuses to change the record.

Section

Subd. 5. Requirements for deleting data in SISs. Requires the enrolling educational institution to delete the data on a student stored in a SIS within one year after the student leaves the institution, except the following data; a student's SSN, records needed to apply to another school or employment, data that is the subject of a formal action or proceeding, aggregated or de-identified data retained for research and analysis, and data required by law or a court.

Subd. 6. Requirements to delete copies of student data. Requires SIS providers and other third parties to delete or destroy physical and digital copies of data on students within 180 days after receiving notice of the student leaving the educational institution, except data that is the subject of a formal action or proceeding, aggregated or de-identified data retained for research and analysis, data required by law or a court, and data retained at the request of the person signing the opt-in agreement and the SIS provider and the educational institution agree to retain the data.

Subd. 7. Notice to SIS provider and third parties. Requires an educational institution to notify the SIS provider, which must then notify affected third parties, within 90 days after a student leaves the educational institution.

Subd. 8. Access under law, judicial warrant, or audit. Denies unauthorized people and entities access to student data unless access is required by law, subject to a warrant, or part an educational institution audit.

Subd. 9. Directory information permitted. Allows an educational institution to provide directory information to vendors for specified purposes if the vendor agrees: not to transmit the data to other third parties; use the data for the purpose specified; and destroy the data after using it.

Subd. 10. Interaction with other law. States that this section does not supersede or limit other student data laws.

4 1-to-1 programs.

Subd. 1. General rule. Prohibits school employees and 1-to-1 device providers and their agents from accessing or tracking students enrolled in a 1-to-1 program who use a 1-to-1 device, except consistent with this section.

Subd. 2. Exceptions. Allows school employees and 1-to-1 device providers and their agents to access data on students enrolled in a 1-to-1 program who use a 1-to-1 device only if: the collected data is not personally identifiable student information; the student's teacher accesses the data for an educational purpose; the school employee or 1-to-1 device provider or its agent is allowed to access personally identifiable student information under an opt-in agreement; a school employee has a reasonable suspicion the student is violating a school policy and the 1-to-1 device contains evidence of the suspected violation, if certain conditions are met; a school employee or law enforcement official reasonably suspects the student is engaging in illegal conduct and the 1-to-1 device contains evidence of the suspected illegal conduct and has a search warrant; access is needed to update or upgrade software or protect the device from cyber-threats; access is needed to respond to an imminent threat to life or safety and the person accessing the device notifies the student, the student's parent, and the

Section

educational institution within 72 hours about the threat and the data accessed; or the information is posted on a publicly accessible Web site or accessible by a school employee given permission by the student to view the content.

Subd. 3. Use of location tracking technology. Prohibits school employees and 1-to-1 device providers and their agents from using the location tracking technology in a student's 1-to-1 device to track the device's real time or historical location unless: such use is subject to a warrant; the student or the student's parent reports the 1-to-1 device is missing or stolen; or such use is needed to respond to an imminent threat to life or safety and the person accessing the device notifies the student, the student's parent, and the educational institution within 72 hours about the threat and the data and features accessed.

Subd. 4. No access to audio or video receiving, transmitting or recording functions; exceptions. Prohibits school employees and 1-to-1 device providers and their agents from activating or accessing audio or video receiving, transmitting or recording functions on a student's 1-to-1 device unless: a student initiates the video or audio chat; the activation or access is subject to a warrant; or such use is needed to respond to an imminent threat to life or safety and the person accessing the device notifies the student, the student's parent, and the educational institution within 72 hours about the threat and the data and features accessed.

Subd. 5. No access to student's password-protected software, Web site accounts, or applications; exceptions. Prohibits school employees and 1-to-1 device providers and their agents from using a 1-to-1 device or requiring a student to use a 1-to-1 device in their presence in order to view a **s**tudent's password-protected software, Web site accounts, or applications except the where the student's classroom teacher views the 1-to-1 device for an educational purpose.

Subd. 6. Prohibited uses of student data. Prohibits school employees and 1-to-1 device providers and their agents from using student data or personally identifiable student information stored on or retrieved from a 1-to-1 device to market or advertise to a student, parent, or school employee, except under an opt-in agreement, or to develop a student profile for any non-educational purpose.

Subd. 7. Training required. Requires school employees to receive training before participating in a 1-to-1 program.

Subd. 8. No sharing of personally identifiable student information; exceptions. Prohibits school employees and 1-to-1 device providers and their agents from transferring personally identifiable student information obtained or received from a 1-to-1 device to another person or entity except to another adequately trained school employee who accesses the information for an educational purpose or to 1-to-1 device provider whose access is authorized under an opt-in agreement.

Subd. 9. Opt-in agreements. (a) Requires opt-in agreements to specify: the information on a student's 1-to-1 device to which access is granted; the name of the school employee or 1-to-1 device provider being granted the access; the educational purpose for granting the access; and the student to whom the agreement applies.

Section

(b) Requires the parent of an elementary or secondary student to sign the opt-in agreement and allows an eligible student to sign the agreement otherwise.

(c) Declared an opt-in agreement invalid if it grants a 1-to-1 device provider general authority to access a student's 1-to-1 device or collect all personally identifiable student information from a program or application.

(d) Allows the party granting access in an opt-in agreement to revoke the agreement at any time and requires the educational institution to notify the 1-to-1 device provider within 30 days.

(e) Places on the 1-to-1 device provider the burden of proving it acted under a valid opt-in agreement.

(f) Prohibits a 1-to-1 device provider from requiring an educational institution or student to use the provider's software or other services in order to use a 1-to-1 device program.

(g) Prohibits an educational institution from withholding a 1-to-1 device or related benefit or punishing a student or parent because of a refusal to sign or a decision to revoke an opt-in agreement or refusal to use a specific service provider.

(h) Prohibits a 1-to-1 device provider from requiring a parent or student to provide personally identifiable student information.

Subd. 10. No sale, sharing, or transfer of personally identifiable student information; exception. Prohibits school employees and 1-to-1 device providers and their agents from transmitting personally identifiable student information to another person or entity except as part of the sale or merger of the 1-to-1 device provider's business. Subjects any buyer of personally identifiable information to the same restrictions and obligations applicable to the seller of the information.

Subd. 11. Direct access prohibited; exceptions. Allows only education institutions, school employees, and 1-to-1 device providers access to a 1-to-1 device and its data unless authorized by law, subject to a warrant, or expressly permitted by the student issued the 1-to-1 device.

Subd. 12. Return of 1-to-1 device; erase data. Requires educational institutions and 1-to-1 device providers to erase and not access data stored by a student on a 1-to-1 device that is permanently returned by the student.

Subd. 13. Personally identifiable student data; general exceptions. Excludes from the effects of this section personally identifiable information 1-to-1 that device providers collect from programs, sites, and applications that were not pre-loaded on a 1-to-1 device and not promoted, marketed, or advertised as part of issuing the device.

5 **Student's personal electronic devices on campus.** (a) Prohibits school employees from accessing or compelling students to provide access to data available through the student's personal technological device, even if the student is carrying it or using the device in violation of a school policy.

(b) Allows a school employee to search a student's personal technological device if the school employee reasonably suspects the student is violating a school policy and the

Section

student's personal technological device has evidence of the suspected violation. Permits the search if: (1) the student's personal technological device is on school property and the school employee documents the reason for the suspicion, notifies the student and the student's parent of the suspected violation and the data to be access in searching for the evidence, limits the search to finding evidence on the violation, and ceases searching upon finding the evidence; or (2) the school employee believes there is an imminent threat to life or safety. Requires school employees and law enforcement officials who access a student's personal technological device in response to an imminent threat to life or safety to inform the student, the student's parent, and the educational institution within 72 hours about the threat that led to accessing the data and the data that was accessed.

(c) Allows an educational institution, subject to applicable laws and restrictions and pending notice, to seize a student's personal technological device to prevent data from being deleted. Limits the pre-notice seizure period to 48 hours. Requires the educational institution to securely store the device on school property and not access the device during the pre-notice period.

(d) Prohibits school employees from transmitting data or information unrelated to the violation leading to a search of a student's personal technological device.

(e) Prohibits searching the personal technological device of a student suspected of illegal conduct unless a law enforcement officer secures a warrant permitting the search.

6 **Limitations on use.** Makes evidence obtained under this act inadmissible in civil or criminal proceedings, disciplinary actions, or administrative hearings.

7 **Penalties.** (a) Subjects people who violate this act to legal actions for damages or equitable relief. Entitles a person injured under this act to actual damages, including pain and suffering and attorney fees.

(b) Subjects school employees who violate this act or an implementing rule or regulation to disciplinary proceedings and punishment. Gives effect to the applicable provisions of this act except where they conflict with a collective bargaining agreement or other agreement or practice applicable to school employees who are members of a bargaining unit.

8 **Severability.** Makes the provisions of this act severable so that if some of the sections or the application of the sections are held invalid, the remaining sections and the application of those sections remain in effect.

9 **Effective date.** Makes sections 1 to 8 effective January 1, 2017.