



Senate Fiscal Agency
P. O. Box 30036
Lansing, Michigan 48909-7536

BILL



ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986

Senate Bill 510 (as enrolled)
Sponsor: Senator Phil Pavlov
Senate Committee: Education
House Committee: Education

Date Completed: 12-21-16

RATIONALE

Educators, students, and parents require data collected from students in order to improve education programs and outcomes. Data allow educators to personalize academic programs, give parents tools to hold schools accountable for performance, and ensure that states allocate appropriate funding for effective programs. The disclosure of data collected for these purposes is limited and regulated under Federal law; however, some have expressed concern that those protections do not adequately safeguard data collected at schools. To address this concern, it has been suggested that additional protections against the disclosure and use of data collected from pupils should be implemented.

CONTENT

The bill would create the "Student Online Personal Protection Act" to establish certain prohibitions and requirements that would apply to an "operator", which would mean the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and is designed and marketed for those purposes. Specifically, the proposed Act would do the following:

- Prohibit an operator from knowingly engaging in certain targeted advertising, using information gathered by the operator to amass a student profile, or selling a student's information.**
- Prohibit an operator from knowingly disclosing covered information, unless the disclosure were made for certain purposes.**
- Require an operator to implement appropriate security procedures and practices, and protect covered information from unauthorized access, destruction, or use.**
- Allow an operator to disclose a student's covered information if required by law or for legitimate research purposes, or if the information were disclosed to a State or local educational agency for K-12 school purposes.**
- Specify that the Act would not prohibit an operator from using covered information to improve or demonstrate the effectiveness of its educational products or services.**
- Provide that the Act would not limit certain activities or abilities of various parties.**

The Act would take effect 90 days after its enactment.

Definitions

"Covered information" would mean personally identifiable information or material in any media or format that is any of the following: a) created by or provided to an operator by a student, or the student's parent or legal guardian, in the course of the student's, parent's, or legal guardian's use of the operator's site, service, or application for K-12 school purposes; b) created by or provided to an operator by an employee or agent of a K-12 school or school district for K-12 school purposes; or c) gathered by an operator through the operation of a site, service, or application for K-12 school purposes and personally identifies a student, including information in the student's

educational record or e-mail, first and last name, home address, telephone number, e-mail address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, Social Security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

"K-12 school purposes" would mean purposes that are directed by or that customarily take place at the direction of a K-12 school, teacher, or school district or aid in the administration of school activities, including instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school. Other than advertising, K-12 school purposes also would include those purposes related to K-12 students preparing for postsecondary education.

"Operator" would mean, to the extent that it is operating in this capacity, the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and is designed and marketed for K-12 school purposes.

"School district" would mean a school district, intermediate school district, or public school academy, as those terms are defined in the Revised School Code.

"Targeted advertising" would mean presenting an advertisement to a student where the advertisement is selected based on information obtained or inferred from that student's online behavior, usage of applications, or covered information. The term would not include advertising to a student at an online location based on that student's current visit to that location or single search query without the collection and retention of a student's online activities over time.

Operator Restrictions & Requirements

An operator would be prohibited from knowingly doing any of the following:

- Engaging in targeted advertising on the operator's site, service, or application, or target advertising on any other site, service, or application if the targeting were based on any information, including covered information and persistent unique identifiers, that the operator had acquired because of the use of its site, service, or application for K-12 school purposes.
- Using information, including persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a student except in furtherance of K-12 purposes.
- Selling or renting a student's information, including covered information.

"Amass a profile" would not include the collection and retention of account registration records or information that remained under the control of the student, the student's parent or guardian, or K-12 school.

The prohibition against selling or renting information would not apply to the purchase, merger, or other type of acquisition of an operator by another entity, if the operator or successor entity complied with the requirements of the proposed Act regarding previously acquired student information.

An operator also would be prohibited from knowingly disclosing covered information, except as otherwise provided, unless the disclosure were made for the following purposes: a) in furtherance of the K-12 school purpose of the site, service, or application, if the recipient of the covered information disclosed did not further disclose it except to allow or improve operability and functionality of the site, service, or application; b) to ensure legal and regulatory compliance or protect against liability; c) to respond to or participate in the judicial process; d) to protect the safety or integrity of the site or others or the security of the site, service, or application; or e) for

a school, educational, or employment purpose requested by the student or the student's parent or guardian, provided that the information was not used or further disclosed for any other purpose.

An operator also could disclose covered information to a service provider, if the operator contractually prohibited the provider from using any covered information for any purpose other than providing the contracted service to or on behalf of the operator, prohibited the service provider from disclosing covered information provided by the operator to subsequent third parties, and required the service provider to implement and maintain reasonable security procedures and practices. This provision would not prohibit the operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application. ("Service provider" would mean a person or entity that provides a service that enables users to access content, information, electronic mail, or other services offered over the internet or a computer network.)

An operator would be required to implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information, and protect that covered information from unauthorized access, destruction, use, modification, or disclosure. An operator also would have to delete a student's covered information if the K-12 school or school district requested deletion of covered information under the control of the K-12 school or school district.

Allowed Disclosure, Use of Covered Information

An operator would be permitted to use or disclose a student's covered information if Federal or State law required the operator to disclose the information, and the operator complied with the requirements of Federal and State law in protecting and disclosing that information. Disclosure also would be allowed for legitimate research purposes as required by State or Federal law and subject to the restrictions under applicable State and Federal law or as allowed by State or Federal law and under the direction of a K-12 school, school district, or state department of education, if covered information were not used for advertising or to amass a profile on the student for purposes other than K-12 school purposes. In addition, an operator could disclose covered information to a State or local educational agency, including K-12 schools and school districts, for K-12 school purposes, as permitted by State or Federal law.

These provisions would not prohibit an operator from: a) using covered information that was not associated with an identified student within the operator's site, service, or application or other sites, services, or applications owned by the operator to improve educational products; b) using covered information that was not associated with an identified student to demonstrate the effectiveness of the operator's products or services, including in their marketing; c) sharing covered information that was not associated with an identified student for the development and improvement of educational sites, services, or applications; or d) responding to a student's request for information or for feedback to help improve learning without the information or response being determined in whole or in part by payment or other consideration from a third party.

The above provisions also would not prohibit an operator from using recommendation engines to recommend to a student additional content or services relating to an educational, other learning, or employment opportunity purpose within the operator's site, service, or application, if the recommendation were not determined in whole or in part by payment or other consideration from a third party.

Scope of the Act

The proposed Act would not do the following:

- Limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or under a court order.
- Limit the ability of an operator to use student data, including covered information, for adaptive learning or customized student learning purposes.

- Apply to general audience internet websites, online services, online applications, or mobile applications, even if login credentials created for an operator's site, service, or application could be used to gain access to those general audience sites, services, or applications.
- Limit service providers from providing internet connectivity to schools or students and their families.
- Prohibit an operator of an internet website, online service, online application, or mobile application from marketing educational products directly to parents if the marketing did not result from the use of covered information obtained by the operator through the provision of services covered under the Act.
- Impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with the Act on those applications or software.
- Impose a duty upon a provider of an interactive computer service to review or enforce compliance with the Act by third-party content providers.
- Prohibit students from downloading, exporting, saving, or maintaining their own student-created data or documents.

The proposed Act also would not prohibit a K-12 school, school district, operator, or service provider from using a student's information, including covered information, solely to identify or display information to the student about or facilitate connection of the student with a not-for-profit institution of higher education or a scholarship opportunity if the K-12 school or school district had first obtained the express written consent of the student's parent or legal guardian or, if the student were age 18 or older or an emancipated minor, the student. For this purpose, express written consent could be obtained as a response to the annual notice required under 34 CFR 99.7 and would not have to be in addition to consent given in response to that notice. (Under 34 CFR 99.7, educational agencies or institutions must notify the parent of a student, or an eligible student, annually of his or her rights under the Family Educational Rights and Privacy Act, including the right to: a) inspect the student's records, b) seek amendment of inaccurate or misleading records, and c) and consent to disclosure of personally identifiable information contained in the records.)

"Interactive computer service" would mean that term as defined in 47 USC 230: any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet and such systems operated or services offered by libraries or educational institutions.

BACKGROUND

As mentioned above, Federal law contains a variety of limitations on the collection and disclosure of information pertaining to students. These include various provisions of the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA). An overview of these laws is provided below.

Family Educational Rights and Privacy Act

The Act and the regulations promulgated under it apply to any educational agency or institution that receives funds from any program administered by the U.S. Department of Education. Under FERPA, parents of pupils under 18 and eligible students are granted certain rights with respect to education records. (An "eligible student" is a student who has reached the age of 18 or a student who is attending a postsecondary institution at any age.)

Specifically, a pupil's parent or an eligible student may inspect and review the student's education records maintained by a school within 45 days of his or her written request, and may request that a school correct inaccurate or misleading records. Generally, FERPA requires schools to have written permission from a parent or eligible student in order to release any information from a student's education record, with certain exceptions. Schools may disclose education records without consent to various parties, for example: a) school officials with legitimate educational interest; b) other schools to which a student is transferring; c) specified officials for evaluation purposes; d) appropriate parties in connection with financial aid; e) accrediting organizations; f) organizations conducting studies for the school; and g) appropriate officials in cases of health and

safety emergencies or in connection with the juvenile justice system.¹ A school also may disclose education records in order to comply with a judicial order or subpoena.

In addition, FERPA allows a school to disclose, without consent, so-called "directory information", or "information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed".² This information can include the student's name, address, phone number, e-mail address, photograph, date and place of birth, major field of study, height and weight, awards, and when the student attended the school.³ The school must inform parents and eligible students about the types of information the school has designated as directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information without prior consent.⁴

The Protection of Pupil Rights Amendment (PPRA) to FERPA further requires that instructional material be available for inspection by a parent or guardian of a child.⁵ Also, under the PPRA, a student cannot be required to submit to a survey or evaluation that reveals information concerning various protected topics without the written consent of a parent or guardian, or in the case of an emancipated or adult student, the student. The protected topics include: a) political affiliations or beliefs, b) mental or psychological problems, c) sex behavior or attitudes, d) illegal or self-incriminating behavior, e) critical appraisals of close family relationships, f) legally protected or privileged relationships (e.g., with lawyers, physicians, or clergy), g) religious practices or beliefs, and h) income (other than that required to determine eligibility for financial assistance). The PPRA requires local educational agencies (schools, school districts, and school boards) to develop policies pertaining to student privacy, student and parent access to information, the collection and use of student personal information for marketing purposes, and the administration of surveys and examinations, including physical examinations.

Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act provides additional protection to children. (This Act defines "child" as an individual under the age of 13.) The Act and its regulations prohibit unfair or deceptive practices in connection with the collection, use, and disclosure of a child's personal information. Specifically, it is unlawful for an operator of a website or online service directed to children, or an operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations promulgated under the Act.⁶ "Personal information" means individually identifiable information about an individual collected online, including, for example, a first and last name, home address, a Social Security number, a telephone number, or a persistent identifier used to recognize a user over time and across different websites (e.g., an Internet Protocol address). The Act also includes express preemptory language: "No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter [Chapter 91-Children's Online Privacy Protection] that is inconsistent with the treatment of those activities or actions under this section."

Under the regulations, an operator must provide notice on the website or online service of what information it collects from children, how much it uses the information, and its practices for disclosure of the information.⁷ In many instances, operators are required to obtain verifiable parental consent before collecting, using, or disclosing a child's personal information. Operators are prohibited from conditioning a child's participation in a game or another activity, or the offering of a prize, on the disclosure of more information than is reasonably necessary to participate in the activity. Further, the regulations require operators to safeguard the confidentiality, integrity, and

¹ 34 C.F.R. § 99.31.

² 34 C.F.R. § 99.3.

³ 34 C.F.R. § 99.3; 20 U.S.C. § 1232g(a)(5)(A).

⁴ 34 C.F.R. § 99.37; 20 U.S.C. § 1232g(a)(5)(B).

⁵ 20 U.S.C. § 1232h.

⁶ 15 U.S.C. § 6502(a)(1).

⁷ The regulations prescribing the notice, parental consent procedures, and other required aspects of COPPA are found at 16 CFR §§ 312.3-312.8.

security of information collected from children, and to ensure that information is disclosed only to third parties who are capable of maintaining its security and confidentiality.

Industry groups and others may apply to the Federal Trade Commission for approval of self-regulatory program guidelines.⁸ These programs must contain performance standards, including: a) requirements that operators provide substantially the same or greater protections for a child's personal information than those provided for by regulations, b) mandatory mechanisms for independent assessment of the operator's compliance with the self-regulatory program, and c) disciplinary actions for an operator's noncompliance with the self-regulatory program guidelines. If approved by the Commission, self-regulatory program guidelines function as a "safe harbor" for operators. Accordingly, an operator will be deemed to be in compliance with COPPA's regulations if it complies with Commission-approved guidelines.

ARGUMENTS

(Please note: The arguments contained in this analysis originate from sources outside the Senate Fiscal Agency. The Senate Fiscal Agency neither supports nor opposes legislation.)

Supporting Argument

These days, education is being conducted online more than ever, and vast amounts of data can easily be collected, stored, and shared. School systems and educators rely increasingly on data to assess student progress as well as for educational research and other purposes. It is possible that these data could be purchased for the purpose of marketing products to students, or stolen for a variety of reasons. Students, parents, and educators deserve an environment in which they can use digital learning tools without fear that any data collected from their use will be manipulated to market products or services or for unethical or illegal purposes. The bill would prevent operators of websites, online services, and applications from using student data to develop targeted advertising and selling or disclosing the information to third parties unless required for a legitimate reason. The bill would balance the need to collect important student information with the need to prevent the collection of student data from becoming an enterprise.

Response: The bill could be improved in several ways. It should provide a framework for student privacy without unnecessarily limiting the ability of students, parents, and educators to use data and technology. Parents and students should have the ability to decide which uses of personal information they consider appropriate and to approve the use or disclosure of personal information, and the bill should prescribe a mechanism for giving approval.

In addition, the bill's language pertaining to the ability of operators to disclose covered information to service providers, as long as those service providers adhered to certain requirements, is unclear. As defined in the bill, "service provider" refers to an internet service provider and not a subcontractor, although a subcontractor typically would be used to deliver educational services. Furthermore, the bill would prohibit the disclosure of covered information by service providers to subsequent third parties. The bill should apply these provisions to subcontractors, instead of internet service providers, and allow subcontractors to disclose covered information to other parties, provided that disclosure was necessary to fulfill educational purposes, and the third parties adhered to the same requirements as imposed on service providers/subcontractors.

Legislative Analyst: Jeff Mann

⁸ Self-regulatory program guidelines and "safe harbor" programs are regulated under 16 CFR § 312.

A1516/s510ea

This analysis was prepared by nonpartisan Senate staff for use by the Senate in its deliberations and does not constitute an official statement of legislative intent.

FISCAL IMPACT

The bill would have no fiscal impact on State or local government.

Fiscal Analyst: Cory Savino

A1516\sb510ea

This analysis was prepared by nonpartisan Senate staff for use by the Senate in its deliberations and does not constitute an official statement of legislative intent.