SENATE COMMITTEE ON EDUCATION
Carol Liu, Chair
2013-14 Regular Session

BILL NO:	SB 1177		
AUTHOR:	Steinberg		
INTRODUCED:	February 20, 2014		
FISCAL COMM:	No	**HEARING DATE:**	March 26, 2014
URGENCY:	No	**CONSULTANT:**	Lenin Del Castillo

NOTE: This bill has been referred to the Committees on Education and Judiciary. A "do pass" motion should include referral to the Committee on Judiciary.

SUBJECT: Student Online Personal Information Protection Act.

SUMMARY

This bill prohibits K-12 online educational sites, services, and applications from compiling, sharing, or disclosing student personal information and from facilitating, marketing, or advertising to K-12 students.

BACKGROUND

Existing law provides that, among other rights, all people have an inalienable right to pursue and obtain privacy. (California Constitution, Article I, Section 1)

Existing law also allows a person to bring an action in tort for an invasion of privacy and provides that in order to state a claim for violation of the constitutional right to privacy, the following three elements must be established:

1) Legally protected privacy interest;

2) Reasonable expectation of privacy in the circumstances; and

3) Conduct by the defendant that constitutes a serious invasion of privacy. (*Hill v. National Collegiate Athletic Association* (1994) 7 Cal.4th 1)

Existing law provides that there is no reasonable expectation of privacy in information posted on an Internet Web site. (*Moreno v. Hanford Sentinel* (2009) 172 Cal.App.4th 1125) Additionally, federal law requires an operator on an Internet Web site or online service that has actual knowledge that it is collecting personal information from a child to provide notice of what information is being collected and how that information is being used, and to give the parents of the child the opportunity to refuse to permit the operator's further collection of information from the child. (15 United States Code, 6502)

Existing law requires an operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual

consumers residing in California who use or visit its Web site to conspicuously post its privacy policy. (Business & Professions Code Section 22575)

Existing federal law makes it unlawful for an operator of a Web site or online service directed to children under the age of 13 to collect personal information from a child, including a child's first and last name, home or other physical address including street name and name of a city or town, e-mail address, telephone number, or Social Security number. (15 U.S.C. Section 6501 et. seq.)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. Section 1232g; 34 CFR Part 99) protects the privacy of student education records. It applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions
(34 CFR Section 99.31):

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, and date and place of birth. However, schools must tell parents and eligible students about directory information and allow them a reasonable amount of time to request that the school not disclose such information. Schools must also notify parents and eligible students annually of their rights under FERPA.

ANALYSIS

This bill:

1) Requires an operator of an Internet Web site, online service, online application, or mobile application used for and designed and marketed for K-12 school purposes to comply with all of the following:

    a) Shall not use, share, disclose, or compile personal information about a K-12 student for any purpose other than the K-12 school purpose and for maintaining the integrity of the site, service, or application.

b) Shall not use, share, disclose, or compile a student's personal information for any commercial purpose, including, but not limited to, advertising or profiling.

c) Shall not allow, facilitate, or aid in the marketing or advertising of a product or service to a K-12 student on the site, service, or application.

d) Shall take all reasonable steps to protect the data at rest and in motion in a manner that meets or exceeds commercial best practices. An operator shall be deemed to be in compliance with this paragraph if the operator ensures valid encryption processes for data at rest and for data in motion, as specified.

2) Requires an operator of an Internet Web site, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for or designed and marketed for K-12 school purposes to provide a notice to the operator of a secondary site, service, or application that is accessible through the noticing operator's site, service, or application that the secondary site, service, or application is used for K-12 school purposes.

3) Requires an operator to comply with this section upon either receiving notice that the site, service, or application is used for K-12 school purposes or if the operator otherwise has actual knowledge that the site, service, or application is used for K-12 school purposes.

4) Requires an operator that fails to provide the notice to be liable for the secondary site, service, or application's compliance with this section, unless that secondary site, service, or application had actual knowledge it was being used for K-12 purposes and was designed and marketed for K-12 school purposes.

5) Requires an operator to delete a student's personal information if any of the following occurs:

a) The site, service, or application is no longer used for the original K-12 school purpose.

b) The student requests deletion, unless it is being used at the direction of a school or district for legitimate educational purposes and is under the control of the school or district.

c) The student ceases to be a student at the institution and the operator becomes aware the student is no longer a student, unless it is being used at the direction of a school or district for legitimate educational purposes and is under the control of the school or district.

6) Provides that an operator may disclose personal information of a student if other provisions of federal or state law require the operator to disclose the information, and the operator complies.

7) Provides that an "online service" includes cloud computing services.

8) Provides that an operator of an Internet Web site, online service, online application, or mobile application used for and designed and marketed for K-12 school purposes may disclose personal information of a student for legitimate research purposes as required by state and federal law and subject to the restrictions under state and federal law.

9) Defines "personal information" as any information or materials in any media or format created or provided by a student or the student's parent or legal guardian, as specified.

10) Provides that these provisions shall not be construed to limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

11) Provides that it is not the intent of the Legislature for this chapter to apply to general audience Internet Web sites.

12) Provides that the provisions of the bill are severable, as specified.

STAFF COMMENTS

1) Author's statement: "The Student Online Personal Information Protection Act ("SOPIPA") closes loopholes that can be exploited by Internet companies for profit through collecting and sharing students' personal information obtained through online services marketed for school purposes.

These companies are operating with zero restrictions, except for the ones that they themselves deem unilaterally appropriate. That is unacceptable. Kids are in the classroom to learn and we value the security of their personal information above private profit.

Many companies provide online services to aide classroom teaching but they require students to create accounts that capture contact data and personal academic information such as grades, disciplinary history, and chat records. In some instances, companies are mining data from schoolchildren beyond the needs of the classroom. Some Apps marketed to teachers and kids could track a child's physical location.

In many cases, the only agreement about how a student's personal information is processed is the privacy policy drafted by the online company. Some privacy policies state that they are "subject to change" unilaterally and at any time.

Others include provisions which affirmatively state that the online company has no liability if they mishandle personal information.

Current federal and state law puts the onus only on schools and school districts to protect student personal information, not online companies. The type of personal information that these companies may gather is broad and highly prized by online advertisers and marketers.

SOPIPA would prohibit the commercial use of student personal information for any secondary purposes including advertising, require online companies to properly encrypt student data, and require deletion of student personal information in certain instances.

We must get ahead of this problem before it's too late. I intend to put safeguards around student personal information while allowing the industry to continue innovating."

2) New era of digital technology in schools. Recent advances in technology have changed the landscape of education in schools and have resulted in the expansion of student data. School districts are increasingly integrating the use of computers and tablets in the classroom to instantly deliver personalized content, employ virtual forums for interacting with other students and teachers, and utilize other interactive technologies to enhance student learning. These technologies, which may be provided directly by school districts and through the use of private contractors and subcontractors, have the potential to transform the classroom and learning processes. Online forums are used to assist teachers with sharing lesson plans and web-based applications help teachers with customized learning experiences for individual students. With access to personal student level education records, these new technologies raise questions concerning the security of this information. To illustrate, the United States Department of Education established the Privacy Technical Assistance Center (PTAC) as a resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. The PTAC recently released new guidance to help schools and educators understand the major laws and best practices protecting student privacy while using online educational services. This guidance summarized the requirements of the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA) that relate to these educational services, and urged school districts to go beyond compliance to follow best practices for outsourcing school functions using online educational services, including computer software, mobile applications, and web-based tools. The author's office indicates that this guidance lends support for why the bill is necessary to place restrictions on the online sites, services, and applications from using student personal information for secondary non-educational purposes and from serving up advertisements while students work online.

3) Smarter Balanced Assessments. California joined the Smarter Balanced Assessment Consortium (SBAC) as a governing state in 2011 for the purpose of developing assessments that are aligned to the common core standards. California committed to administering the SBAC assessments to pupils beginning in the 2014-15 school year. SBAC will develop an assessment system with major deliverables that include online computer adaptive summative assessments that give a snapshot of student performance without a "one size fits all approach" and an online tailored reporting system that provides educators access to information about students' progress toward college and career readiness as well as students' specific strengths and weaknesses along the way. The State Department of Education indicates that it does not believe the bill's provisions will impact the SBAC assessments.

4) Definition of K-12 school purposes? As the bill moves forward, the author may wish to address several issues worth consideration. While the bill is intended to prevent the use of student information for secondary purposes such as advertising and marketing, it does not define "K-12 school purposes." Therefore the bill could be interpreted to have broad application and raise some level of ambiguity. For example, would the provisions of the bill apply to social media or general purpose Internet sites that may have some K-12 instructional nexus but are not exclusively used for K-12 purposes? Further, if disputes arise, who is the enforcement agency that would rule on such matters? Without a clear definition of "K-12 school purposes", the bill's provisions could potentially impact general audience Internet sites.

5) Related and prior legislation. This bill is similar to Senate Bill 568 (Steinberg), Chapter 336, Statutes of 2013, which requires operators of online sites, services, and applications to allow minors to remove what they post and also prohibits these operators from serving up advertisements to minors for products and services minors cannot legally purchase in California, such as alcohol, tobacco, and firearms.

SUPPORT

Common Sense Media
Klaas Kids Foundation
Privacy Rights Clearinghouse
Services Employees International Union

OPPOSITION

None on file.