SB2607

Measure Title:	RELATING TO STUDENT DATA MANAGEMENT.
Report Title:	Student Data; Computer Services
Description:	Limits the ways in which the operator of a website, online service, online application, or mobile application working with the DOE can use student data.
Companion:	HB1712
Package:	None
Current Referral:	EDU/EET, JDL
Introducer(s):	KIDANI, DELA CRUZ, HARIMOTO, NISHIHARA, WAKAI, Shimabukuro

DAVID Y. IGE
GOVERNOR

KATHRYN S. MATAYOSHI
SUPERINTENDENT

STATE OF HAWAI`I
DEPARTMENT OF EDUCATION
P.O. BOX 2360
HONOLULU, HAWAI`I 96804

Date: 02/05/2016
Time: 01:00 PM
Location: 229
Committee: Senate Education Senate Economic Development, Environment, and Technology

Department: Education

Person Testifying: Kathryn S. Matayoshi, Superintendent of Education

Title of Bill: SB 2607 RELATING TO STUDENT DATA MANAGEMENT.

Purpose of Bill: Limits the ways in which the operator of a website, online service, online application, or mobile application working with the DOE can use student data.

Department's Position:
The Department of Education supports the intent of S.B. No. 2607 to protect student information and offers the following comments

· Several provisions of the bill allow for the disclosure of information for purposes of improving the operator's site, service, or application. It is unclear what types of covered information would be disclosed for those purposes. In particular, page 7, lines 3-6 states:

"Nothing in this section shall prohibit the operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application."

The Department is concerned that this language may be overly broad in allowing access to student information.

· Page 9, lines 3-10 refer to "covered information that is not associated with an identified student." The Department finds this language contradictory, as a student must be "identified" when referring to "covered information."

· Page 11, lines 10-17 appear to absolve certain providers from enforcing

compliance with this law on applications or software, or by third-party content providers. The Department is concerned that these provisions limit responsibility at the expense of student data privacy.

Thank you for the opportunity to testify on S.B. No. 2607.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

February 4, 2016

Senator Michelle N. Kidani, Chair
Committee on Education

Senator Glenn Wakai, Chair
Committee on Economic Development, Environment, and Technology

RE: S.B. 2607, Relating to Student Data Management
Hearing – Friday, February 5, 1:00 pm, Room 229

Dear Chair Kidani, Chair Wakai, Members of the Joint Committees:

Microsoft has been an early leader in the area of student data privacy, and is in **strong support** of S.B. 2607, which limits the ways in which the operator of an educational website, online service, online application, or mobile application can use student data. We believe that this measure will address privacy concerns and strengthen trust in educational technologies by eliminating commercial practices that do not belong in the classroom. At the same time, the bill will enable innovation by allowing the use of student data to provide personalized learning and develop new educational technologies that can improve education and help students learn. In summary, this bill will:

- Require clear and easy-to-understand policies on the collection, retention, use and any sharing of student personal information;
- Prohibit school service providers from selling student personal information
- Prohibit school service providers from creating a personal profile of a student other than for educational purposes;
- Prohibit any use or sharing of student data for purposes of behaviorally targeting advertisements to students; and
- Require providers to maintain a comprehensive information security program with appropriate administrative, technological and physical safeguards.

A growing number of states around the country (including most recently California, Arkansas, Delaware, Georgia, Kentucky, Maine, Maryland, New Hampshire, Oregon, and Washington) have passed laws that would provide safeguards to students in the classroom. Importantly, the language in S.B. 2607 represents consensus language that has evolved as laws have passed in other states, and has been supported by education groups, advocates and major technology companies.

1. Privacy Concerns About the Increasing Collection of Student Data by Technology Companies

Schools have undergone a technological revolution, and are bringing a range of beneficial online services and technologies into the classroom. That includes a range of beneficial technologies that operate in "the cloud" (i.e., online), including productivity tools such as email and document storage, as well as online tutoring programs and tools to help track student progress. Bringing cloud services into schools has led to the collection of large amounts of data by the technology companies that provide such services. In turn, that has led to serious privacy concerns.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

A growing range of stakeholders from around the country have become concerned that there are insufficient safeguards in place to prevent technology companies from using data about K-12 students for commercial purposes that have no relation to education. For example, many schools have been found to provide cloud service providers with access to substantial amounts of student data without adequate protections to prevent the data from being used for commercial purposes unrelated to education. According to a recent study by Fordham University Law School's Center on Law and Information Policy, schools "frequently surrender control of student information when using cloud services."[1] Fewer than 25% of school contracts with cloud computing companies specify the purposes for which student data may be disclosed, and fewer than 7% of such contracts restrict the sale or marketing of student data by companies. The overwhelming majority of these contracts fail to address parental notice, consent, or access to student information.

2. Existing Federal Laws Do Not Protect Student Data

Federal laws governing student data have failed to address the rise of cloud computing technology. Two laws that opponents of student privacy legislation often cite as protecting students, the Family Educational Rights and Privacy Act ("FERPA")[2] and the Children's Online Privacy Protection Act ("COPPA"),[3] have significant gaps that can enable cloud computing providers to misuse student data for commercial purposes unrelated to education, like advertising.

FERPA is four decades old and is ill-suited to address the rising tide of cloud computing. Significantly, FERPA applies to the disclosure of "personally identifiable information" ("PII") in student "education records," but as the U.S. Department of Education recently confirmed in new FERPA guidance,[4] much of the data that cloud computing companies use for advertising purposes is not covered. FERPA also lacks teeth because it can be enforced only against educational institutions, not cloud computing companies.[5] Moreover, because FERPA applies only to schools that receive funding from the Department of Education, it does not apply to most private and parochial schools.[6]

COPPA similarly fails to adequately address the protection of student data that is processed by cloud computing providers. COPPA applies to operators of websites or online services, but only applies to children under the age of 13, and not to high schools. COPPA establishes a robust privacy framework for some contexts, but it has significant limitations when applied to cloud computing services in schools. Recent revisions to the COPPA Rule did not on their face address how COPPA applies to schools and

---

[1] Joel R. Reidenberg et al., *Executive Summary - Privacy and Cloud Computing in Public Schools*, CENTER ON LAW AND INFORMATION POLICY AT FORDHAM LAW SCHOOL, p. 1 (Dec. 12, 2013), *available at:* http://law.fordham.edu/assets/CLIP/Privacy_and_Cloud_Computing_-_EXECUTIVE_SUMMARY_-_FINAL%282%29.pdf.

[2] *See* 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

[3] *See* 15 U.S.C. §§ 6501-6506; 16 C.F.R. Part 312.

[4] *See FERPA General Guidance for Parents*, U.S. DEPT. OF EDUCATION, (last visited Feb. 26, 2014), *available at:* http://www2.ed.gov/policy/gen/guid/fpco/ferpa/parents.html

[5] *See* Daniel Solove, *Why Schools Are Flunking Privacy and How They Can Improve*, SAFEGOV, (Dec. 16, 2013), *available at:* http://www.safegov.org/2013/12/16/why-schools-are-flunking-privacy-and-how-they-can-improve.

[6] *See generally FERPA General Guidance for Parents*, U.S. DEPT. OF EDUCATION, (last visited Feb. 26, 2014), *available at:* http://www2.ed.gov/policy/gen/guid/fpco/ferpa/parents.html.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

students.[7] Although the Federal Trade Commission ("FTC") staff has addressed COPPA's application to schools in a set of Frequently Asked Questions published on its website, this informal guidance is not a regulation and its reach can be called into question.[8]

Even with primary schools, there is considerable confusion about how and when parental consent must be obtained under COPPA. Schools are not deeply familiar with online advertising practices and thus are ill-equipped to grapple with COPPA, especially when cloud providers are not transparent about their data practices.

3. Parents, Advocates, and Academics Are Concerned

Parents overwhelmingly are opposed to companies using student data for unrelated commercial purposes. In a 2013 survey conducted by SafeGov, 75% of parents expressed disapproval of vendor practices that included using student data for marketing or advertising purposes.[9] 92% of parents agreed that schools should require such companies "to offer a privacy policy expressly designed for school children that provides strict guarantees against user profiling or web tracking."[10] Common Sense Media[11] and other advocacy groups have supported prohibitions on using student data for commercial purposes, such as advertising and marketing.

For the above reasons, we strongly support S.B. 2607 and respectfully request that the Committee pass this measure. Thank you for your consideration and for the opportunity to submit testimony on this bill.

Respectfully submitted,

Jonathan Noble
Director, State and Local Government Affairs
US Government Affairs
Microsoft Corporation

---

[7] *See* Children's Online Privacy Protection Act Rule, 78 Fed. Reg. 3972 (Jan. 17, 2013).

[8] *See Complying with COPPA: Frequently Asked Questions*, FTC, (last visited Feb. 26, 2014), *available at*: http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions.

[9] *SafeGov 2012 National Data Privacy in Schools Survey*, SAFEGOV, p. 6 (Jan. 2013), *available at:* http://safegov.org/media/43502/brunswick_edu_data_privacy_report_jan_2013.pdf.

[10] *Id.* at 9.

[11] *See* Natasha Singer, *Group Presses for Safeguards on the Personal Data of Schoolchildren*, N.Y. TIMES (Oct. 13, 2013), *available at:* http://www.nytimes.com/2013/10/14/technology/concerns-arise-over-privacy-of-schoolchildrens-data.html?_r=0; Jim Steyer, *Why We Need Safeguards to Protect Kids' Data*, COMMON SENSE MEDIA (Oct. 14, 2013), *available at:* http://www.commonsensemedia.org/blog/why-we-need-safeguards-to-protect-kids-data.