



STATE OF HAWAII
DEPARTMENT OF EDUCATION
P.O. BOX 2360
HONOLULU, HAWAII 96804

Date: 02/03/2016
Time: 02:00 PM
Location: 309
Committee: House Education

Department: Education

Person Testifying: Kathryn S. Matayoshi, Superintendent of Education

Title of Bill: HB 1712 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:

Department's Position:

The Department of Education supports the intent of H.B. No. 1712 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 H.B. No. 1712.

DAVID Y. IGE
GOVERNOR



CATHERINE PAYNE
CHAIRPERSON

STATE OF HAWAII
STATE PUBLIC CHARTER SCHOOL COMMISSION
(‘AHA KULA HO‘ĀMANA)

<http://CharterCommission.Hawaii.Gov>
1111 Bishop Street, Suite 516, Honolulu, Hawaii 96813
Tel: (808) 586-3775 Fax: (808) 586-3776

FOR: HB 1712 Relating to Student Data Management
DATE: Wednesday, February 3, 2016
TIME: 1:15 PM
COMMITTEE(S): Senate Committee on Education
ROOM: Conference Room 229
FROM: Tom Hutton, Executive Director
State Public Charter School Commission

Comments on HB 1712

Chair Takumi, Vice Chair Ohno, and members of the Committee:

The State Public Charter School Commission appreciates the opportunity to submit these comments. This proposal may be intended to apply to the Department of Education, but when proposed legislation addresses “public schools,” this includes public charter schools. If that is not the intent, we respectfully request that the bill be amended to refer specifically to “department schools.” If the intent is to include public charter schools, the Commission supports the intent of protecting student information and privacy but has some concerns as to how this bill would require public schools to comply.

Thank you for the opportunity to provide this testimony.

Attached is testimony for HB 1712 Relating to Student Data Management:

Testifier: Jonathan Noble, Director, State & Local Government Affairs, Microsoft Corporation

Position: Support

Committee Hearing: EDN

Hearing Date: February 3, 2016

Hearing Time: 2:00 pm

Testifier will be present.

February 2, 2016

Representative Roy Takumi, Chair
House Committee on Education

RE: H.B. 1712, Relating to Student Data Management
Hearing – Wednesday, February 3, 2:00 pm, Room 309

Dear Representative Takumi and Members of the Committee on Education:

Microsoft has been an early leader in the area of student data privacy, and is in **strong support** of H.B. 1712, 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 H.B. 1712 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.

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 students.⁷ Although the Federal Trade Commission ("FTC") staff has addressed COPPA's application to

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](http://law.fordham.edu/assets/CLIP/Privacy%20and%20Cloud%20Computing%20-%20EXECUTIVE%20SUMMARY%20-%20FINAL%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>.

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

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 Media¹¹ 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 H.B. 1712 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

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.common sense media.org/blog/why-we-need-safeguards-to-protect-kids-data>.

HB1712

Submitted on: 2/1/2016

Testimony for EDN on Feb 3, 2016 14:00PM in Conference Room 309

Submitted By	Organization	Testifier Position	Present at Hearing
cheryl	Individual	Support	No

Comments: How are we limiting? Do you know how much data has already gone out and being used by companies like Pearson, Tripod Survey people, Google, Kid Biz, Reading Plus, Springboard to name just a few? Every time our kids log on in the DOE they are being tracked It is important to limit this totally and to relook at how much data the DOE REALLY needs to help our kids be successful. As a retired teacher, I know that my in class data collection was all that I needed to help my kids

Please note that testimony submitted less than 24 hours prior to the hearing, improperly identified, or directed to the incorrect office, may not be posted online or distributed to the committee prior to the convening of the public hearing.

Do not reply to this email. This inbox is not monitored. For assistance please email webmaster@capitol.hawaii.gov