

February 23, 2016

Senator Gilbert S.C. Keith-Agaran, Chair
Senate Committee on Judiciary and Labor

RE: S.B. 2607, S.D.1, Relating to Student Data Management

Dear Senator Keith-Agaran and Members of the Committee on Judiciary and Labor:

Microsoft has been an early leader in the area of student data privacy, and is in **strong support** of S.B. 2607, S.D.1, 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, S.D.1, 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_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>.

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.

4. Suggested amendments for consideration

Microsoft has been in ongoing discussions with the Hawaii State Department of Education regarding this measure. We would note that the amendments to the language in the S.D.1 version of the bill were the result of those discussions, with recognition that the language might need to be fine-tuned. Based upon our most recent discussion, we would ask that the following amendments originally made in the S.D.1 be removed from the bill:

- Remove the language, on page 11, lines 11 – 13: “provided that the applications and software companies shall make a good faith effort to protect covered information”
- Remove the language, on page 11, lines 17-19: “provided that the third party content provider shall make a good faith effort to protect covered information”

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>.

These proposed amendments would remove language that would otherwise unintentionally weaken the responsibility of third party content providers, applications and software companies to comply with the bill and protect the privacy of student data.

We strongly support S.B. 2607, S.D.1 and respectfully request that the Committee pass this measure, with the changes noted above. Thank you for your consideration and for the opportunity to submit testimony on this bill.

Respectfully submitted,

Ryan Harkins
Director, State Affairs and Public Policy
US Government Affairs
Microsoft Corporation

From: mailinglist@capitol.hawaii.gov
To: [JDLTestimony](#)
Cc:
Subject: Submitted testimony for SB2607 on Feb 25, 2016 09:01AM
Date: Tuesday, February 23, 2016 9:51:28 PM

SB2607

Submitted on: 2/23/2016

Testimony for JDL on Feb 25, 2016 09:01AM in Conference Room 016

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

Comments: Do you even know the ways that Pearson and other companies are using the data which they gather on our children? Each time our children log on to a program (which they do daily now with Wonders and Springboard, Kid Biz, Reading Plus and more) their information is taken and used in ways we still don't know. Then there's the SBA and Tripod.. It goes on endlessly. PLEASE stop them.

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

From: mailinglist@capitol.hawaii.gov
To: [JDLTestimony](#)
Cc:
Subject: *Submitted testimony for SB2607 on Feb 25, 2016 09:01AM*
Date: Tuesday, February 23, 2016 9:56:49 PM

SB2607

Submitted on: 2/23/2016

Testimony for JDL on Feb 25, 2016 09:01AM in Conference Room 016

Submitted By	Organization	Testifier Position	Present at Hearing
Rachel L. Kailianu	Individual	Support	Yes

Comments:

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