

March 20, 2016

Representative Angus McKelvey, Chair  
House Committee on Consumer Protection & Commerce

**RE: S.B. 2607, S.D.2, Relating to Student Data Management  
Hearing – Monday, March 21, 2016, 3:00 p.m., Room 325**

Dear Representative McKelvey and Members of the Committee on Consumer Protection & Commerce:

Microsoft has been an early leader in the area of student data privacy, and is in **strong support** of S.B. 2607, S.D.2, 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.2, 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."<sup>1</sup> 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")<sup>2</sup> and the Children's Online Privacy Protection Act ("COPPA"),<sup>3</sup> 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,<sup>4</sup> 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.<sup>5</sup> 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.<sup>6</sup>

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

---

<sup>1</sup> 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).

<sup>2</sup> See 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

<sup>3</sup> See 15 U.S.C. §§ 6501-6506; 16 C.F.R. Part 312.

<sup>4</sup> 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>

<sup>5</sup> 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>.

<sup>6</sup> 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>.

students.<sup>7</sup> 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.<sup>8</sup>

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.<sup>9</sup> 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.”<sup>10</sup> Common Sense Media<sup>11</sup> and other advocacy groups have supported prohibitions on using student data for commercial purposes, such as advertising and marketing.

Microsoft has been in ongoing discussions with the Hawaii State Department of Education regarding this bill, and notes that the current draft of the bill reflects the consensus between the parties regarding this measure.

We strongly support S.B. 2607, S.D.2 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,

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

---

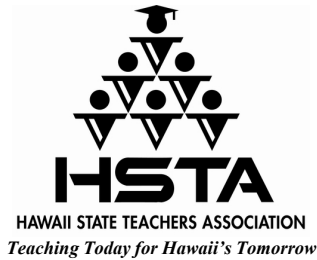
<sup>7</sup> See Children’s Online Privacy Protection Act Rule, 78 Fed. Reg. 3972 (Jan. 17, 2013).

<sup>8</sup> 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>.

<sup>9</sup> *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](http://safegov.org/media/43502/brunswick_edu_data_privacy_report_jan_2013.pdf).

<sup>10</sup> *Id.* at 9.

<sup>11</sup> 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](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>.



1200 Ala Kapuna Street \*\* Honolulu, Hawaii 96819  
Tel: (808) 833-2711 \*\* Fax: (808) 839-7106 \*\* Web: www.hsta.org

Corey Rosenlee  
President  
Justin Hughey  
Vice President  
Amy Perruso  
Secretary-Treasurer  
Wilbert Holck  
Executive Director

TESTIMONY BEFORE THE HOUSE COMMITTEE ON CONSUMER  
PROTECTION & COMMERCE

RE: SB 2607, SD2 - RELATING TO STUDENT DATA MANAGEMENT.

MONDAY, MARCH 21, 2016

COREY ROSENLEE, PRESIDENT  
HAWAII STATE TEACHERS ASSOCIATION

Chair McKelvey and Members of the Committee:

The Hawaii State Teachers Association **supports SB 2607, SD2**, relating to student data management.

Under existing federal law, the Federal Educational Rights and Privacy Act (FERPA) generally seeks to protect the confidentiality of educational records (and personally identifiable information contained therein) by prohibiting the funding of schools that permit the release of those records. (20 U.S.C. Sec. 1232g(b)(1).) FERPA's prohibition only applies to the school itself and contains various exemptions where the data may be released without the written consent of the parents. Since the enactment of FERPA in 1974, educational institutions have undergone dramatic changes in the way that students are taught, including the increased use of technology.

In response to the increased use of technology in the classroom, this bill seeks to prohibit the 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.

Although at HSTA we value technology and online programs, we must ensure our students are protected. SB 2607 SD2 is a positive step that will assist with this goal by setting limits on the information that online companies can use, store, and/or share. It is vital that we protect our students from unsolicited advertisements, as well as many other uses that their data could be used for, instead of just providing their teachers and parents with information that would assist them in reaching their learning targets.

We appreciate the language of the bill, and the deletion of lines in the previous draft that would have weakened the intent of this bill to protect our students and their data.

To protect our keiki from data mining and to ensure their data is kept private and only used for the purposes intended, the Hawaii State Teachers Association asks your committee to **support** this bill.



March 21, 2016

Senator Michelle Kidani, Chair  
Committee on Education

Representative Roy Takumi, Chair  
Committee on Education

Representative Angus McKelvey, Chair  
Committee on Consumer Protection and Commerce

Dear Chair Kidani, Chair Takumi, Chair McKelvey:

ACT, Inc. is a national nonprofit organization whose mission is to help people achieve education and workplace success. This memo details our concerns with pending legislation relating to personal student information.

ACT responsibly uses all of the data it collects, balancing data's potential to help students with the need to ensure student privacy and confidentiality. In recognition of this deep responsibility to students and the vital role that information and information security play for ACT and its education partners, ACT follows a strict and transparent program to safeguard data owned by or entrusted to ACT. ACT's privacy policy can be found online at <http://www.act.org/privacy.html>.

ACT commends efforts at both the state and federal levels to provide much-needed updates to antiquated privacy laws that allow far too many loopholes regarding access to and sharing of data. However, new legislation designed to prevent operators from disclosing and/or misusing student data often defines these operators in ways that will impede ACT's ability to continue providing students, policymakers, postsecondary institutions, and the general public with valuable services or useful information about the state of education in the U.S.

Specifically, because registration for the ACT test is now being offered online, and the test itself (and eventually all ACT assessment solutions) will soon also be administered online, ACT interprets the definition of "operator" as applying to ACT as well as to other similar nonprofit educational assessment and research companies—applications that seem to run counter to the bill author's intent.

This results in unintended consequences of the new legislation in at least three areas:

**1. Delivering ACT's Educational Opportunity Service**

To help students receive information about educational, scholarship, career, and postsecondary financial aid information, ACT, with student consent, will disclose data to accredited postsecondary institutions and scholarship services via its Educational Opportunity Service (EOS). If a student chooses to participate in EOS, the following information from the student's ACT test registration form becomes available to participating organizations that pay a small processing fee per student: name, address, gender, high school, email address, birthdate, expected year of high school graduation, racial/ethnic background (if provided by the student), intended college major, and occupational preference. Through EOS, ACT has helped millions of students find higher education and financial aid opportunities that match their goals, many of which they would have been unaware of without EOS.

The legislation prohibits an operator from selling student information to any entity regardless of whether or not the student consented to the sale for that purpose. ACT recommends that the legislation be revised to permit operators to sell covered information when documentation of student consent exists.

## **2. Retaining student data to conduct longitudinal research**

For more than 56 years, ACT has collected data via the ACT test about the academic readiness of high school graduates for college-level coursework in English, math, reading, and science. The science behind ACT's assessments—the evidence base and ongoing research—relies on ACT's ability to collect and analyze these data and is critical in answering the key question of what matters most in helping people to succeed in education and work.

In addition to developing student assessments, ACT also promotes education and workforce policy solutions at the national, state, and local levels. We provide policymakers with researchbased insights—largely using reports based on aggregated student assessment data—to inform their policy decisions. For example, ACT has published a series of Catching Up to College and Career Readiness reports that aggregate de-identified student data to underscore the importance and explore the challenges of getting and keeping students on target for college and career readiness. Each year, ACT also publishes The Condition of College & Career Readiness for each state and the nation. These reports highlight the progress of each year's ACT-tested graduating class toward college and career readiness, again using only aggregated, deidentified student data.

Thus, data are critical to refining and strengthening ACT's assessment solutions and informing educational institutions' efforts to ensure that all students progress toward postsecondary and workplace success.

The legislation requires operators to delete a student's covered information if the school or district requests deletion of data under the control of the school or district. While ACT research reports do not publish covered information, ACT must use the covered data to conduct the analyses that it does publish in de-identified form. ACT recommends that the legislation be revised to permit operators to keep covered information for research purposes, provided that the covered information is never shared in public reports unless de-identified and aggregated.

## **3. Conducting educational research separate from the direction of the state or district**

Language in the legislation subjects educational research to the direction of the state or a district or school. This approach assumes that only states, districts, or schools should generate research proposals, thus depriving students and the general public of research expertise by universities, nonprofit organizations such as ACT, and other similar repositories of knowledge.

While the legislation provides that information may be used for "legitimate research purposes [. . .] as allowed by state or federal law," it also limits this provision to research conducted under the direction of a school or a state department. ACT recommends that the legislation be revised to permit operators such as ACT to perform research activities independent of state and school directives as long as only de-identified aggregated information is reported publicly.

The Honorable Roy M. Takumi, the Honorable Michelle N. Kidani, the Honorable Angus McKelvey

March 21, 2016

Page 3 of 3

To ensure that student data privacy legislation does not prevent nonprofit organizations such as ACT from delivering important information to students and the public, we appreciate your consideration of the discussion above. If you have any questions or concerns, please contact Scott Frein at (202) 223-2318 or [scott.frein@act.org](mailto:scott.frein@act.org). Thank you.

Sincerely,

A handwritten signature in blue ink, appearing to read "S. Montgomery", with a long horizontal flourish extending to the right.

Scott Montgomery

Vice President

Policy, Advocacy, and Government Relations

ACT, Inc.



# LATE TESTIMONY

DAVID Y. IGE  
GOVERNOR



KATHRYN S. MATAYOSHI  
SUPERINTENDENT

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

**LATE**

**Date:** 03/21/2016  
**Time:** 03:00 PM  
**Location:** 325  
**Committee:** House Consumer Protection and  
Commerce

**Department:** Education

**Person Testifying:** Kathryn S. Matayoshi, Superintendent of Education

**Title of Bill:** SB 2607, SD2 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. Takes effect on 1/7/2059. (SD2)

**Department's Position:**  
The Hawaii Department of Education (HIDOE) supports the intent of S.B. NO. 2607, which it believes is in line with its efforts to aggressively protect student privacy. Additionally, HIDOE is governed by privacy policies of the U.S. Department of Education for families, Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act of 1998, Hawaii Administrative Rule §8-34 Protection of Educational Rights and Privacy of Students and Parents, and Board of Education Policy 4610 which limit the use and disclosure of identifiable student information.