

# HB613 HD1

Measure Title: RELATING TO STUDENT DATA MANAGEMENT.

Report Title: Student data; Computer services

Description: Limits and controls the ways in which a computer service provider working with the DOE can use student data. (HB613 HD1)

Companion:

Package: None

Current Referral: EDU, CPN

Introducer(s): EVANS, TAKUMI

<u>Sort by Date</u>		<b>Status Text</b>
1/23/2015	H	Pending introduction.
1/26/2015	H	Introduced and Pass First Reading.
1/28/2015	H	Referred to EDN, JUD, referral sheet 2
2/9/2015	H	Bill scheduled to be heard by EDN on Wednesday, 02-11-15 2:00PM in House conference room 309.
2/12/2015	H	The committees on EDN recommend that the measure be PASSED, UNAMENDED. The votes were as follows: 10 Ayes: Representative(s) Takumi, Ohno, Choy, Ing, Kong, LoPresti, Say, Tsuji, Matsumoto, Tupola; Ayes with reservations: none; Noes: none; and 3 Excused: Representative(s) Aquino, Ichiyama, Ito.
2/20/2015	H	Reported from EDN (Stand. Com. Rep. No. 431), recommending passage on Second Reading and referral to JUD.
2/20/2015	H	Passed Second Reading and referred to the committee(s) on JUD with none voting aye with reservations; none voting no (0) and Ito excused (1).
3/2/2015	H	Bill scheduled to be heard by JUD on Thursday, 03-05-15 2:00PM in House conference room 325.
3/5/2015	H	The committees on JUD recommend that the measure be PASSED, WITH AMENDMENTS. The votes were as follows: 13 Ayes: Representative(s) Rhoads, San Buenaventura, Brower, Creagan, Hashem, Kawakami, C. Lee, Morikawa, Nakashima, Takayama, Woodson, McDermott, Thielen; Ayes with reservations: none; Noes: none; and 1 Excused: Representative(s) Belatti.
3/6/2015	H	Reported from JUD (Stand. Com. Rep. No. 844) as amended in HD 1, recommending passage on Third Reading.
3/6/2015	H	Forty-eight (48) hours notice Tuesday, 03-10-15.

3/10/2015	H	Passed Third Reading as amended in HD 1 with none voting aye with reservations; none voting no (0) and Jordan, McDermott excused (2). Transmitted to Senate.
3/12/2015	S	Received from House (Hse. Com. No. 212).
3/12/2015	S	Passed First Reading.
3/12/2015	S	Referred to EDU, CPN.
3/12/2015	S	The committee(s) on EDU has scheduled a public hearing on 03-16-15 1:15PM in conference room 229.



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

TESTIMONY BEFORE THE SENATE COMMITTEE  
ON EDUCATION

Wil Okabe  
President  
Joan Kamila Lewis  
Vice President  
Colleen Pasco  
Secretary-Treasurer  
Wilbert Holck  
Executive Director

DATE: MONDAY, MARCH 16, 2015

RE: H.B. 613, H.D. 1 – RELATING TO STUDENT DATA MANAGEMENT

PERSON TESTIFYING: JOAN LEWIS, VICE PRESIDENT  
HAWAII STATE TEACHERS ASSOCIATION

The Honorable Chair Michelle Kidani, Honorable Vice Chair Breene Harimoto and Members of the Committee:

The Hawaii State Teachers Association (HSTA) **supports H.B.613, H.D. 1**, relating to student data management.

HSTA is the exclusive representative of more than 13,500 public and charter school teachers statewide. As the state affiliate of the 2.2 million member National Education Association (NEA), per the 2014 HSTA Digest of Policy Statements and New Business Items 2014 handbook, HSTA believes that parents and students should be informed and protected from unsolicited data mining, and informed of their rights to opt-out of personal information release.

Thank you for the opportunity to testify.

**Testimony of  
Gary M. Slovin / Mihoko E. Ito/ Rick Tsujimura  
on behalf of  
Microsoft**

DATE: March 15, 2015

TO: Senator Michelle N. Kidani  
Chair, Committee on Education  
*Submitted Via [EDUTestimony@capitol.hawaii.gov](mailto:EDUTestimony@capitol.hawaii.gov)*

RE: **H.B. 613, HD1 – Relating to Student Data Management**  
**Hearing Date: Monday, March 16, 2015 at 1:15 p.m.**  
**Conference Room: 229**

---

Dear Chair Kidani and Members of the Committee on Education:

We submit this testimony on behalf of Microsoft. Microsoft **supports the intent** of H.B. 613, HD1, which protects student privacy by limiting the ways in which a computer service provider working with the DOE can use student data. Microsoft has been involved as one of the first companies to sign the Student Privacy Pledge and to recognize the need to treat sensitive student data in the same way that we treat other enterprise data, such as government, health or financial services data. The company has been a strong supporter of creating more consistent and uniform state legislation to protect the privacy of student data.

We would suggest that other national models, such as the SUPER Act described below, might be considered if the Committee is inclined to move this measure forward. H.B. 613, HD1 in its current form requires schools to ensure adequate safeguards are in place about how their service providers disclose and use the data. This measure will be a key part of protecting student privacy and ensuring that student data is not misused by computer service providers for commercial purposes unrelated to education.

Parents, advocates, and academics increasingly are concerned about data security issues for their children and believe that reform is needed to safeguard student data from being sold or misused for inappropriate commercial purposes when it is transferred from schools to computer service providers. (See *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) )

We encourage this Committee to adopt a more uniform approach to the law, and have attached the SUPER Act, which many states are now considering. The Virginia Legislature most recently passed similar legislation. The language is based on the Student Privacy Pledge and

---

Gary M. Slovin  
R. Brian Tsujimura  
Mihoko E. Ito  
C. Mike Kido  
Tiffany N. Yajima

999 Bishop Street, Suite 1400  
Honolulu, HI 96813  
(808) 539-0840

endorsed by President Obama and signed by over 40 companies, including Microsoft, Google, Apple and others, who commit to safeguarding student privacy.

The language of the SUPER Act would:

- Require clear and easy-to-understand policies on the collection, retention, use and any sharing of student personal information;
- Ensure student data is only used for authorized purposes by the educational institution, teacher, student and/or parent;
- Prohibit school service providers from selling student personal information and from creating a personal profile of a student other than for purposes authorized by educators or with appropriate consent;
- Prohibit any use or sharing of student data for purposes of behaviorally targeting advertisements to students;
- Require providers to maintain a comprehensive information security program with appropriate administrative, technological and physical safeguards; and
- Require any third parties involved on the school service providers' behalf to adhere to the obligations of the act.

Many states have recognized that the federal laws governing student data are outdated and inadequate. One such law, the Family Educational Rights and Privacy Act (“FERPA”) was passed in 1974, well before the rise of new technologies like cloud computing. The protections provided by the law have failed to keep pace with technology and have gaps that can permit student data collected from schools to be used for commercial practices that have no relation to education, like targeted advertising.

Specifically, FERPA applies only to “personally identifiable information” in a student’s “education records,” and there is a growing range of data collected by online services about students that doesn’t fall within those definitions. It also applies to education institutions, not to online services, and cannot be enforced directly against technology companies. FERPA also contains exemptions that permit the disclosure of personally identifiable information in education records under certain circumstances, and some have interpreted those exemptions as permitting the use of student data for purposes like targeted advertising.

Another federal law, the Children’s Online Privacy Act, similarly fails to solve the specific challenges raised by cloud computing to the protection of student data. COPPA applies to operators of websites or online services that are directed to children under the age of 13 and to operators that have actual knowledge that they collect personal information from children under 13. Consequently, COPPA does not apply to high school students. 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. Although the Federal Trade Commission 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.

We appreciate the opportunity to testify, and respectfully request consideration of the model act language to be included in this measure.

## Student User Privacy in Education Rights Act

### **Section 1. Title.**

This act shall be known and may be cited as the "Student User Privacy in Education Rights Act" or "SUPER Act".

### **Section 2. Definitions.**

- (1) "Targeted advertising" means sending advertisements to a student where the advertisement is selected based on information obtained or inferred from that student's online behavior, usage of applications, or student personal information. It does not include (a) advertising to a student at an online location based upon that student's current visit to that location without the collection and retention of a student's online activities over time or (b) adaptive learning, personalized learning or customized education.
- (2) "School service" means a website, mobile application, or online service that: (a) is designed and marketed primarily for use in a K-12 school; (b) is used at the direction of teachers or other employees of a K-12 school; and (c) collects, maintains or uses student personal information. A "school service" does not include a website, mobile application, or online service that is designed and marketed for use by individuals or entities generally, even if also marketed to a United States K-12 school.
- (3) "School service provider" means an entity that operates a school service.
- (4) "Students" means students of K-12 schools in the state of Hawaii.
- (5) "Student personal information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that personally identifies an individual student.

### **Section 3. Obligations of School Service Providers: Transparency.**

- (1) School service providers shall provide clear and easy-to-understand information about the types of student personal information they collect and about how they use and share such student personal information.
- (2) School service providers shall provide prominent notice before making material changes to their privacy policies for school services.
- (3) School service providers shall facilitate access to and correction of student personal information by students or their parent or guardian either directly or through the relevant educational institution or teacher.
- (4) Where the school service is offered to an educational institution or teacher, information required by subsections (1) and (2) of this Section 3 may be provided to the educational institution or teacher.

### **Section 4. Obligations of School Service Providers: Choice and Control.**

- (1) School service providers may collect, use, and share student personal information only for purposes authorized by the relevant educational institution or teacher, or with the consent of the student or their parent or guardian.
- (2) School service providers may not sell student personal information. This prohibition does not apply to the purchase, merger, or other type of acquisition of a school service provider, or any assets of a service provider by another entity, provided that the successor entity continues to be subject to the provisions of this section with

respect to previously acquired student information to the extent that the service provider was regulated by this Act with regard to its acquisition of student information.

- (3) School service providers may not use or share any student personal information for purposes of targeted advertising to students.
- (4) School service providers may not use student personal information to create a personal profile of a student other than for supporting purposes authorized by the relevant educational institution or teacher, or with the consent of the student or their parent or guardian.
- (5) School service providers must obtain consent before using student personal information in a manner that is materially inconsistent with the school service provider's privacy policy or school contract for the applicable school service in effect at the time of collection.
- (6) The provisions of paragraphs (1), (2), (4), and (5) shall not apply to use or disclosure of student personal information by a school provider to:
  - (a) Protect the security or integrity of its website, mobile application, or online service;
  - (b) Ensure legal or regulatory compliance, or to take precautions against liability;
  - (c) Respond to or participate in judicial process
  - (d) Protect the safety of users or others on the website, mobile application, or online service;
  - (e) Investigate a matter related to public safety; or
  - (f) To a service provider, provided the school service provider: (i) contractually prohibits the service provider from using any student personal information for any purpose other than providing the contracted service to, or on behalf of, the school service provider; (ii) prohibits the service provider from disclosing any student personal information provided by the school service provider to subsequent third parties unless the disclosure is expressly permitted by paragraphs (a-e) or sections 6 and 7 and (iii) requires the service provider to comply with the requirements of this Act.

### **Section 5. Obligations of School Service Providers: Safeguards.**

- (1) School service providers must maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information. The information security program should make use of appropriate administrative, technological, and physical safeguards.
- (2) School service providers must delete a student's personal information within a reasonable period of time if the relevant educational institution requests deletion of the data under the control of the educational institution unless (a) the school service provider has obtained student consent or the consent of the student's parent or guardian to retain information related to that student, or (b) the student has transferred to another educational institution and that educational institution has requested that the service provider retain information related to that student.

### **Section 6. Adaptive Learning and Customized Education.**

Notwithstanding sections 2 through 7 of this act, nothing in this act is intended to prohibit the use of student personal information for purposes of:

- (1) Adaptive learning, personalized or customized education.
- (2) Maintaining, developing, supporting, improving, or diagnosing the school service provider's website, mobile application, online service or application.



- (3) Providing recommendations for school, educational, or employment purposes within a school service without the response being determined in whole or in part by payment or other consideration from a third party.
- (4) Responding to a student's request for information or for feedback without the information or response being determined in whole or in part by payment or other consideration from a third party.

#### **Section 7.**

Sections 2 through 8 of this act adopt and do not modify existing law regarding consent, including consent from minors and employees on behalf of educational institutions.

#### **Section 8.**

This act shall not be construed to:

- (1) Impose a duty upon a provider of an interactive computer service, as defined in Section 230 or Title 47 of the United States Code, to review or enforce compliance with this section by third-party content providers.
- (2) Apply to general audience Internet websites, general audience mobile applications, or general audience online services even if login credentials created for a school service provider's website, mobile application or online service may be used to access those general audience websites, mobile applications, or online services.
- (3) Impede the ability of students to download, export, or otherwise save or maintain their own student data or documents.
- (4) Limit Internet Service Providers from providing Internet connectivity to schools or students and their families;
- (5) Prohibit a school service provider from marketing educational products directly to parents so long as the marketing did not result from use or student personal information obtained by the school service provider through the provision of its website, mobile application, or online service.
- (6) Impose a duty on a provider of an electronic store, gateway, marketplace or other means of purchasing or downloading software or applications to review or enforce compliance of this section on those applications or software.

#### **Section 9. Effective Date and Transitional Provisions.**

This Act shall come into force on July 1, 2016 .

If a school service provider entered into a signed, written contract with an educational institution or teacher before to the effective date of this section, the school service provider is not liable for the requirements of sections 2 through 6 of this act with respect to that contract until the next renewal date of the contract.

March 13, 2015

The Honorable Michelle Kidani, Chair  
Senate Education Committee  
Hawaii State Capitol, Room 228  
Honolulu, HI 96813

**Re: HB 613 (Evans and Takumi) Student Data Management**

Dear Senator Kidani,

On behalf of the members of TechAmerica, powered by CompTIA, I appreciate the opportunity to share our perspective on House Bill 613 relating to student data management. While the intention of this legislation is to protect student privacy, the overly broad language of the bill will create barriers to first-class education and innovation in the classroom.

TechAmerica, powered by CompTIA, is the leading voice for the U.S. technology industry – the driving force behind productivity growth and job creation in the United States, representing premier technology companies of all sizes.

We appreciate Hawaii's interest in protecting the privacy and use of student data, however HB 613 does not accomplish that goal in a workable fashion. Rather than empower schools and educators to take advantage of technologies to transform learning this bill places obstacles between students and tools that enhance the educational environment. The extremely broad restrictions imposed by the bill would make it unnecessarily difficult for Hawaii's students and educators to reap the growing benefits of the online education space and develop career-ready skills, which far outweighs any of the bill's presumed benefits.

A bill has been introduced in the House, however, that offers the foundation for a balanced approach to achieving world class education outcomes while protecting student privacy. HB 106 builds off of a law that California enacted last year to implement privacy protections. While the tech industry would still like to see some changes to the language in HB 106, we think it provides a better starting point to arrive at the best outcome for Hawaii's students. Many other states are considering similar legislation and harmonizing the competing bills is an important part of ensuring quality education products. A number of our member companies who provide education software and services are working with those states on this language and would be prepared to do the same in Hawaii.

We look forward to continuing to collaborate with you and improve the opportunities and outcomes for all students in Hawaii. If you have any questions, please contact Kelly Hitt at [KHitt@comptia.org](mailto:KHitt@comptia.org) or 916-505-9053.

Thank you,

Kelly Hitt  
Director, State Government Affairs - California and Hawaii TechAmerica

House Committee on Education  
Hawaii State Capitol, Room 229  
March 16, 2015; 1:15 PM  
415 South Beretania St.  
Honolulu, HI 96813

Written Testimony of Jim Halpert

on behalf of the

**State Privacy and Security Coalition, Inc.**

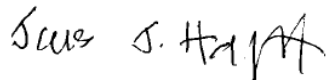
Dear Chair Kidani:

The State Privacy & Security Coalition, which is comprised of 26 leading communications, technology, retail, and media companies, and 6 trade associations, writes to express several concerns regarding to H.B. 613.

This bill would create major obstacles to the use of technology services by schools in Hawaii by prohibiting any disclosure of student data by a service provider for a “commercial purpose.” The result would be to bar commercial service providers from using commercial subcontractors to improve educational services for Hawaii school children. It may also act to prohibit beneficial disclosures by private sector providers of computing services made at the direction of a school, student or parent. Furthermore, although described as a bill about “student data management,” the bill does not address the important issue of security of student data.

Please feel free to contact us at the information below if you have any questions or would like to discuss our concerns in greater detail. Thank you for your time and consideration.

Sincerely,



James J. Halpert  
General Counsel

500 8th Street NW  
Washington, DC 20005  
(202) 799-4000  
[Jim.Halpert@dlapiper.com](mailto:Jim.Halpert@dlapiper.com)



25 Massachusetts Ave., NW  
Washington, DC 20001  
Phone: 202-346-1100

March 14, 2015

Sen. Michelle Kidani  
Chair, Senate Education Committee  
Hawaii State Capitol  
Room 228  
415 South Beretania St.  
Honolulu, HI 96813

Dear Madam Chair:

I am writing in regards to HB 613, a bill that would impose restrictions on the use of “student data” by a “computer service provider.” Rather than empower schools and educators to take advantage of technologies to transform learning, this bill places obstacles between students and tools that enhance the educational environment. The extremely broad restrictions imposed by the bill would make it unnecessarily difficult for Hawaii’s students and educators to reap the growing benefits of the online education tools. We believe that working together, educators and the technology community can provide safe, secure, and powerful new learning environments for all of America’s students. For example, HB 106, though it requires some amendments, is a bill that comes from a better direction in striking the right balance protecting student data and allows for the necessary operation and interaction of online educational services.

While the definitions of the terms defined in HB 613 may have been intended to apply only to a subset of service providers, they are written such that, in reality, *any* online service used by a school could fall into scope, regardless of whether the provider was even aware that the school was using its service. A school could direct students to use a particular site and based on the definition of “computer service provider” that site would likely be “provid[ing] the department with a computer-based service that processes student data” since the bill does not limit applicability only to contracted services and the definition of “process” itself is so broad in scope. Such generality leads to confusion in schools and providers alike.

The bill also does not allow computer service providers to “...disclose, or otherwise process student data for any commercial...purpose.” This restriction is so broad and the term “commercial” so unclear that it calls into question educators’ ability to use services like turnitin.com, a third-party plagiarism checking website or online tutorial sites such as Khan Academy. Sites like these may have relationships with education software vendors that allow users to sign in or utilize the services through their school accounts, but under a strict reading of this bill could be prevented from being utilized by teachers or students in

Hawaii. The intent of this language might be narrow, but its practical application would be stifling.

Because the bill tries to make general and sweeping restrictions that do not account for how online services are used or operate, the consequences can prevent schools, teachers and students from being able to take full advantage of online services and tools that have become integral to education in the 21st century classroom. The approach taken by HB 106 and being similarly considered in a number of states this legislative session, generally offers a much clearer and understandable set of protections and guidelines for the use of student data. For these reasons, I respectfully request that you not advance this bill and instead consider other more workable approaches.

Sincerely,

A handwritten signature in blue ink, appearing to read "Ron Barnes", is centered below the word "Sincerely,".

Ron Barnes  
Head of State Legislative Affairs

**From:**  
**To:** Submitted testimony for HB613 on Mar 16, 2015 13:15PM  
**Cc:** Sunday, March 15, 2015 8:40:21 AM  
**Subject:**  
**Date:**

---

**HB613**

Submitted on: 3/15/2015

Testimony for EDU on Mar 16, 2015 13:15PM in Conference Room 229

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Present at Hearing</b>
James Gauer	Individual	Support	No

Comments: How aware are parents of the information that their children enters through the internet on DOE computers and the risks involved with that information? Sure, parents sign a consent form to allow their child to access and use the internet, but do they really understand how providers can sell or advertise student information to third parties? Support this bill.

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](mailto:webmaster@capitol.hawaii.gov)