Chair Prozanski and members of the Senate Judiciary Committee:

I appreciate the intent of SB 187 A, the "Oregon Student Information Protection Act" (OSIPA). This Act was introduced at the request of Attorney General Ellen Rosenblum. The original bill would have established a task force to make recommendations regarding protection of privacy of students using education software. **I respectfully ask this committee to amend SB 187 A and replace the text with the original language as I think the bill is ambiguously written and unenforceable.**

A privacy advocate, I have closely followed this issue for over three years. This past summer, I attended meetings convened by the Oregon Education Investment Board and I attended the Joint Judiciary informational hearing on December 10th. At that time, AG Ellen Rosenbaum brought Nate Cardozo, staff attorney on the Electronic Frontier Foundation's digital civil liberties team, to talk about the perils of big data. He spent a good portion of his time addressing concerns about Google and the popular Chromebooks.

Around that time, *Education Week* listed the top ten digital education stories of 2014 and Google was #1.

1. Google Under Fire for Data-Mining Student Email Messages
2. InBloom to Shut Down Amid Growing Data-Privacy Concerns
3. 'Landmark' Student-Data-Privacy Law Enacted in California
4. Millions of Student Records Sold in Bankruptcy Case
5. U.S. Education Department Issues Guidance on Student Data Privacy
6. New Guide for District Tech Leaders on Front Lines of Student Privacy Battle
7. Ed. Data-Mining Research Effort Wins Federal Grant, Raises Privacy Questions
8. Push for 'Learner Profiles' Stymied by Barriers
9. Senators Introduce New Federal Data Privacy Legislation
10. Nevada Dad Told It Will Cost $10K to See School Data State Collects on His Children

At the first public hearing of SB 187, -1 amendments were under consideration. AG Rosenblum said, "FERPA is not prepared for the age of big data." She warned that students are "recorded and tracked" on their devices and this monitoring follows them to home. She said, personalized learning "data has real commercial value." She pointed out that the EdTech sector generated $8 billion 2012-13 and is projected to add $300 billion annually in economic activity in coming years.

"Personal information" as Rep. Lew Frederick said in his testimony that day, "is the currency of the 21st Century." Who has sovereignty over their story when everything (test scores, keystrokes, behavior notes, online viewing choices and more) can be recorded and transmitted to the clouds? He says that regulations and the "good will" of data custodians are the only barriers between employers, admission officers, marketers, recruiters and curious eyes getting access to the data; and we can't depend on the good will of data custodians.

AG Rosenblum wants no parental "opt out loophole" to "waive protections" that come with enactment of the bill. She asked the committee to consider a bill modeled on California's

SOPIPA, The Student Online Personal Information Protection Act. She said, "Creating a patchwork quilt of different state statutes places a burden on the EdTech industry, students and policy makers" and that we must "strive for uniformity."

The language of OPIPA is not uniform with SOPIPA.
Both "shall" and "may" are used differently in SOPIPA and OSIPA. For example:

SOPIPA text:

(b) An operator shall not knowingly engage in any of the following activities…

OPIPA text:

(3)(a) An operator may not knowingly engage in any of the following activities…

In legal jargon obligation (shall) is different than authorization (may). "Shall" means that an action is required; the term "may" means that it is permitted but not required. Some, however, argue that "shall" is problematic language and that "may not" means mandatory denial of the right, power, or privilege.

But maybe this is just semantics and the real problem is "knowingly." OPIPA depends on the good will of data custodians to "not knowingly engage" in the very activities this bill is *supposed* to regulate:

- Targeted advertising
- Profiling students
- Selling covered information
- Disclosing information, unless done "(i)n furtherance of the K–12 purpose of the site, service, or application"

This is a huge problem since the bill doesn't specify who is accountable for reading the operators' terms of use. Nor does the bill require the district to post the terms of use.

1. Who determines whether disclosures are "in furtherance of the kindergarten through grade 12 school purposes of the site, service or application"?
2. Will it fall to unsuspecting busy teachers, wooed by EdTech, just as physicians are by pharmaceutical reps with their free samples?
3. Will businesses like Education Framework (based in Bend Oregon) be regulated for the "privacy risk score" they assign to web sites and apps to determine whether parental consent be required or if the software should even be used?
4. Should the education data producer (the student/teacher/school/district) and the data consumer (the operator) come to an agreement before an HTTP transaction takes place with the Accountable Hyper Text Transfer Protocol, HTTPA? This protocol cannot prevent the unauthorized reuse of data, but it can be used to develop accountability mechanisms that will identify violators allowing them to be held accountable for data they inappropriately consumed and served.
5. What would stop operators from using proprietary computer algorithms to surreptitiously profile students for targeted advertising, and to connect the student's profile to the student's home computer? Consider the following in OPIPA:

Nothing in this section shall be construed to limit the authority of a provider of an interactive computer service to review or enforce compliance with this section by third-party content providers.

c) An operator of an Internet website, online service, online application or mobile application from marketing educational products directly to parents or legal guardians, as long as the marketing does not result from the use of covered information obtained by the operator through the provision of services covered under this section;

6. **How can Oregon's Unlawful Trade Practices Act, which has no private right of action, enforce any of the provisions?**

What about health records, maintained as "education records" on internet-based platforms in K-12? The last joint guidance on HIPAA and FERPA was in 2008 *before* FERPA rule changes in 2008 and 2011 broadened exemptions of to disclose education records without consent. The HIPAA privacy rule simply does not apply to most students' health records because the US Department of Health and Human Services has ruled that "individually identifiable health information that is part of an 'education record'... would not be considered protected health information. **This guidance is inadequate, inconsistent, and incomprehensible** in the era of big data, where seemingly infinite bytes of data are collected and shared.

School based health centers (SBHC) are a fast growing initiative in all states. Portland-based Oregon Community Health Information Network (OCHIN) created a graphic to show how FERPA and HIPAA apply. The rules get really messy when school-based health centers bill insurance companies. That's when HIPAA security (but not privacy) rules may (or may not) apply.

As OCHIN explains in this paper, postsecondary institutions exclude medical and psychological treatment records of eligible students from the definition of "education records" if they are made, maintained, and used only in connection with treatment of the student; and disclosed only to individuals providing the treatment. Yet the University of Oregon is the epicenter for FERPA controversy. U of O administrators used a FERPA exemption to access a student's post-rape records without her consent to defend the school against her Title IX lawsuit.

If it's not ok for EdTech operators to profile students, what about school districts? Portland Public School District profiles students as "suicidal" as part of their Suicide Prevention Protocol. The Suicide Protocol is initiated when a student is exhibiting any of the following behaviors: gestures, talk of suicide (including those thoughts expressed in writing, art, or other forms), or suicide attempts. Since the suicide screening form is maintained in the student's cumulative file is it uploaded in the PPS Student Information System, Synergy?

The biggest concern I have with both SOPIPA and OSIPA is what I call the **"Google Exemption Clause."**

(8) Nothing in this section shall be construed to impose a duty upon:

(a) A provider of an electronic store, gateway, marketplace or other means of purchasing or downloading software or applications to review or enforce compliance with this section by those applications or software; or (b) A provider of an interactive computer service to review or enforce compliance with this section by third-party content providers. As used in this paragraph, **"interactive computer service" means any information service, system or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such services or systems operated or offered by libraries or educational institutions.**

(9) This section **does not apply to general audience Internet websites, general audience online services, general audience online applications or general audience mobile applications, even if login credentials created for an operator's site, service or application may be used to access those general audience sites, services or applications**.

School districts across the nation have implemented Google Apps for Education and cloud-based Google Chromebooks because they are free/cheap.

A computer is identified by a "cookie," which is most often specific to an individual browser[1] on that computer.

How unique is your browser? The Electronic Frontier Foundation investigated "the real-world effectiveness of browser fingerprinting algorithms."[2] Up to 94.2% exhibited "instantaneously unique fingerprints" when the EFF used a simple algorithm to guess and follow many fingerprint changes. The authors assert, "Global identifier fingerprints are a worst case for privacy." The EFF identified only three groups of browsers with comparatively good resistance to fingerprinting: those that block JavaScript, those that use TorButton, and certain types of smartphones. Blocking JavaScript (a scripting programming language that makes web pages functional for specific purposes) may limit the content or functionality of a web page unfortunately.

Are you, like me (with Adobe flash and JavaScript enabled; Firefox as a browser; and https and other privacy apps installed), one of the 94.2%? Test yourself at https://panopticlick.eff.org/

Since multiple students access school computers, cookies shouldn't be able to connect browser habits to the individual, right?

Google's got that covered.

Students generally login to Google Chromebooks with their first and last name. Sometimes they login with a Student ID number, a persistent unique identifier. Both data *may* allow Google to track the student as they browse through websites.

With deep pockets, Google invests in all sorts of ventures. One joint investment with the CIA is Recorded Futures for "*Real Time Threat Intelligence.*" Google Apps for Education and their app, Vault could become the Stasi for Schools.
Here are some of "use cases" marketed for Vault:

- *A group of students were accused of bullying another student. However, the students denied the accusation. While going through chat and email records archived in Google Apps Vault, the school dean was able to find evidence of the bullying.*
- *Parents sue a school with 1,000 students. The parents' lawyer asks, in the discovery process, to see all of the email traffic related to their child. In response, the IT Admin of the school can search for related emails in the Vault, including any emails that a member of the staff has deleted.*

In February, the Electronic Privacy Information Center submitted a letter to the House Early Childhood, Elementary and Secondary Education Subcommittee on "How Emerging Technology Affects Student Privacy." Their comprehensive recommendations include enactment of a Student Privacy Bill of Rights, an enforceable student privacy and data security framework, which is based largely based on the well-established Fair Information Practices.

In summary, OPIPA is ambiguous and unenforceable. This benefits the EdTech sector, anxious to stimulate $300 billion of economic activity in the classroom and in the home. Without proof that education technology will improve children's lives, EdTech's marketing magic will surely disinvest more money from the classroom, further ramping up class sizes and narrowing curriculum.

Please convene a task force to implement a strong Student Information Protection Act.
OSIPA fails to put sufficient ethical boundaries on the collection, retention, protection, and use of that data. Data custodians will be able to violate this law because they can.

Parents must have the right to opt their child out of internet-based activities for which there are inadequate privacy/security provisions.

Nearly 100 years ago, the Supreme Court overturned the Oregon Compulsory Public Education, Measure 6 (1922) in deciding Pierce, Governor of Oregon, et al. v. Society of the Sisters of the Holy Names of Jesus and Mary. George E. Chamberlain and Albert H. Putney argued for the governor that the state had an overriding interest to oversee and control the providers of education to the children of Oregon, with one of them calling Oregonian students "the State's children." ‘

The Supreme Court decision states: "The child is not the mere creature of the State; those who nurture him and direct his destiny have the right, coupled with the high duty, to recognize and prepare him for additional obligations."

Respectfully,
Kris Alman MD