April 14, 2015

Senator Floyd Prozanski
Chair, Senate Committee on Judiciary
900 Court St. NE, S-415
Salem, Oregon 97301

Re: SB 187 – Oregon Student Information Protection Act

Dear Chairman Prozanski,

Common Sense Media appreciates Attorney General Rosenblum's and the Oregon Senate's efforts to address Oregon students' privacy with SB 187, the Oregon Student Information Protection Act (OSIPA). Common Sense testified in support of the bill on February 26, 2015. **Since then, however, Common Sense has become concerned that the apparently industry-driven April 8th amendments create new loopholes and weaken OSIPA's protections for students. We respectfully urge you to restore and strengthen the bill, so Oregon students have the protections they deserve and can use educational technology with trust that their personal information won't be exploited or fall into the wrong hands.**.

Oregon schools are increasingly integrating computers, laptops, and tablets in the classroom, and relying on cloud computing services for a variety of academic and administrative functions. This technology, used wisely, has the potential to enhance and personalize student learning and to improve school efficiency. To realize this promise, we must ensure that students' personal information is protected. Through online platforms, mobile applications, digital courseware, and cloud computing, educational technology providers collect massive amounts of sensitive data about students – including contact information, performance records, online activity, health information, behavior and disciplinary records, eligibility for free or reduced-price lunch – even cafeteria selections and whether or not students ride the bus to school. This personal student information is at risk.

Some online services have collected and analyzed personal details about students without clear limits on use of the student data for educational purposes.[1] Other online services have failed to adequately secure and encrypt students' personal information from potential misuse.[2] In fact, a study by Fordham Law School's Center on Law and Information Policy found that the majority of school district cloud service agreements have serious deficiencies in the protection of student information, "generally do not provide for data security and even allow vendors with alarming frequency to retain student information in perpetuity."[3] The more vendors share this data with others, particularly without clear rules, the more vulnerable this data becomes.

---

[1] *See, e.g.*, Benjamin Herold, *Google Under Fire for Data-Mining Student Email Messages*, Education Week (Mar. 13, 2014), http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html?cmp=ENL-EU-NEWS2.

[2] Natasha Singer, *Data Security Gaps in an Industry Pledge,* New York Times Bits Blog (Feb. 11, 2015), http://bits.blogs.nytimes.com/2015/02/11/data-security-gaps-in-an-industry-student-privacy-pledge/?ref=topics; Natasha Singer, *Uncovering Security Flaws in Digital Education Products for Schoolchildren,* New York Times (Feb. 8, 2015).

[3] Press Release, *Fordham Law National Study Finds Public School Use of Cloud Computing Services Causes Data Privacy Problems* (Dec. 13, 2013), http://law.fordham.edu/32158.htm; Natasha Singer*, Schools Use Web Tools, and Data is Seen at Risk,* New York Times (Dec. 12, 2013).

The bill we supported on February 26 would have provided strong protections to safeguard and secure students' sensitive data. It would have **prohibited** K-12 websites, online services, and mobile applications from:

- o using students' personal information for targeted advertising to students or families;
- o using students' personal information for commercial profiling;
- o selling students' personal information; and
- o disclosing students' personal information (except in limited circumstances as provided).

In addition, it would have required these online companies to implement reasonable security for students' personal information, and to delete the information upon the school's request. The measure would have applied to a broad range of K-12 directed websites, services, and apps, whether or not under contract.

The original OSIPA was based on a landmark California law, the Student Online Privacy and Information Protection Act (SOPIPA), which **passed unanimously** through both chambers of the California Legislature and was signed into law in September 2014. The California bill went through an extensive legislative process, with robust input from industry and other stakeholders. The result was a balanced bill that provided strong protection for students while permitting industry innovation and research.

The April 8 amendments to Oregon's OSIPA are problematic and chip away protections for Oregon schoolchildren. Some of the most concerning changes include:

- The amended definitions for "covered information," "Kindergarten through grade 12 school purposes," and "operator" all serve to narrow coverage, weaken protection, and create uncertainty.

- The amendments broadly permit service providers to disclose covered student personal information for "Kindergarten through grade 12 school purposes," without any downstream restrictions for the recipients' use or subsequent disclosure. Once disclosed, students' sensitive information could be used, shared and data-mined without limit.

  The new definition of targeted ads is also problematic, including because it would permit companies to data mine and exploit students' sensitive information to market to parents, who can be particularly vulnerable to ads purporting to provide them with tools to "help" their kids. This amendment would be akin to permitting companies to troll children's medical records so they can market purported health remedies directly to the patients' parents, when medical professionals should be the gatekeepers who can provide expert guidance.

- It is unclear why other amendments are necessary and without clarification they simply serve to confuse, not create a trusted online learning environment. An amendment permitting "a student-initiated request" is extremely vague and open-ended, and it is unclear what (or whose) purposes this serves. There also appears to be broadening of permitted disclosure of student information in Section 6. All these amendments can be viewed as creating new loopholes.

Finally, we note that there seems to be a drafting error in Section 5(a), which should not be a standalone clause; as written it would permit broad disclosure of sensitive student information.

We urge you to reject the recent amendments to SB 187 and to create clear rules to prevent companies from misusing sensitive student information. We are available to discuss in more detail and look forward to working with you to resolve the above concerns.

Simply put, the school zone should be a privacy zone, a safe and trusted environment where our kids can learn and explore, where educators can harness technology to enrich their learning, and where their sensitive information is safe and secure.

Respectfully submitted,

James P. Steyer
Founder and CEO
Common Sense Media

Cc: Attorney General Ellen F. Rosenblum