



January 19, 2016

Senator Steve Abrams, Chair; - Senate Education Committee  
Representative Ron Highland; Chair – House Education Committee

**RE: Kansas Student Privacy Bill**

I am writing on behalf of Microsoft to applaud your consideration of legislation to protect the privacy of data about K-12 students collected by technology companies in Kansas schools. Kansas should join the growing number of states around the country that have passed laws that would drive certain practices out of the classroom—practices like using data about K-12 students for targeted advertising or to create profiles of students for non-educational purposes—and increase trust in beneficial technologies that can provide personalized learning and improve education.

**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,<sup>1</sup> as well as online tutoring programs and tools to help track student progress.<sup>2</sup> 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.

Indeed, 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>3</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

---

<sup>1</sup> See, e.g., Microsoft Office 365 Education, available at: <http://office.microsoft.com/en-us/academic/> (last visited Feb. 26, 2014); Google Apps for Education, available at: <http://www.google.com/enterprise/apps/education/> (last visited Feb. 26, 2014).

<sup>2</sup> See, e.g., Nulu, available at: <http://www.nulu.com/> (last visited Feb. 26, 2014) (providing cloud-based language education tools); Uzinggo, available at: <http://www.uzinggo.com/> (last visited Feb. 26, 2014) (providing online tutoring); Edmodo available at: <http://www.edmodo.com/about> (last visited Feb. 26, 2014) (providing a range of cloud-based teaching tools).

<sup>3</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).



marketing” of student data by companies.<sup>4</sup> In addition, the “overwhelming majority” of contracts fail to “address parental notice, consent, or access to student information.”<sup>5</sup>

## **2. 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>6</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>7</sup>

Common Sense Media<sup>8</sup> and other advocacy groups have supported prohibitions on using student data for commercial purposes, such as advertising and marketing. Academics have expressed similar sentiments. For example, Daniel Solove, a renowned law professor in this field, has observed that schools are “[t]he greatest threat to children’s privacy” and he has called for new regulations to protect student privacy and increased enforcement against vendors.<sup>9</sup> Professor Joel Reidenberg, the lead author of the Fordham study, also has advocated for restrictions on the use of student data for commercial purposes.<sup>10</sup>

## **3. Existing Federal Laws Do Not Protect Student Data**

Federal laws governing student data have failed to address the rise of cloud computing technology. In fact, two laws that opponents of student privacy legislation often cite as protecting students, the Family Educational Rights and Privacy Act (“FERPA”)<sup>11</sup> and the Children’s Online Privacy Protection Act

(“COPPA”),<sup>12</sup> have significant gaps that can enable cloud computing providers to misuse student data for commercial purposes unrelated to education, like advertising.

---

<sup>4</sup> *Id.*

<sup>5</sup> *Id.* at 2.

<sup>6</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>7</sup> *Id.* at 9.

<sup>8</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>.

<sup>9</sup> 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>10</sup> See, e.g., Statement of Joel R. Reidenberg in the General Assembly of Maryland in a Hearing before the Ways and Means Committee on H.B. 607, the Education-Student Privacy and Cloud Computing Act (Feb. 21, 2014).

<sup>11</sup> See 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

<sup>12</sup> See 15 U.S.C. §§ 6501-6506; 16 C.F.R. Part 312.



FERPA is four decades old and is ill-suited to address the rising tide of cloud computing. As Professor Solove has noted, FERPA is “extremely vague about cloud computing” and “very permissive in allowing data sharing to cloud computing providers.”<sup>13</sup> Other limitations further undermine FERPA’s effectiveness. Significantly, FERPA applies to the disclosure of “personally identifiable information” (“PII”) in student “education records,” but as the Department of Education recently confirmed in new FERPA guidance,<sup>14</sup> much of the data that cloud computing companies use for advertising purposes does not constitute “PII” under the statute.<sup>15</sup> It also is not clear that such data is even found in student “education records.” FERPA also lacks teeth because it can be enforced only against educational institutions, not cloud computing companies, and the only penalty available — the withholding of all federal funding from a state or from schools within a state — is so draconian that it has never been levied.<sup>16</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>17</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 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. COPPA establishes a robust privacy framework for some contexts,<sup>18</sup> 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.<sup>19</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>20</sup>

COPPA also is deficient because it does not apply to children 13 or older, and thus cannot apply to high schools. 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.

#### **4. Lawmakers Are Concerned and Are Acting**

---

<sup>13</sup> Daniel Solove, *FERPA and the Cloud: Why FERPA Desperately Needs Reform*, LINKEDIN (Dec. 11, 2012), available at: <http://www.linkedin.com/today/post/article/20121211124311-2259773-ferpa-and-the-cloud-why-ferpa-desperately-needs-reform?trk=mp-author-card>.

<sup>14</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>15</sup> See 34 C.F.R. § 99.3.

<sup>16</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>17</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>.

<sup>18</sup> See generally 16 C.F.R. Part 312.

<sup>19</sup> See Children’s Online Privacy Protection Act Rule, 78 Fed. Reg. 3972 (Jan. 17, 2013).

<sup>20</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>.



In response, U.S. states are passing laws to ensure that technology companies who are invited into schools will use data about students for authorized educational purposes, and not for targeted advertising or creating student profiles for non-educational purposes, like providing credit or insurance. California passed a landmark student privacy law last year,<sup>21</sup> the Student Online Personal Information Protection Act (SOPIPA). Since then, a number of states have passed their own versions of SOPIPA, each containing modest revisions that will help avoid unintentionally inhibiting innovative educational technologies while ensuring that the privacy of student information is protected.<sup>22</sup> That trend promises to continue. According to the Data Quality Campaign, 110 student privacy bills were introduced in states around the country in 2014, followed by over 180 bills introduced in 2015.

## 5. Conclusion

Microsoft has been an early leader on this issue. We have supported the passage of new student privacy laws at the state and federal levels. We were a founding signatory of a [Student Privacy Pledge](#),<sup>23</sup> which was created last fall by members of the education technology industry and two industry associations, the Future of Privacy Forum and the Software and Information Industry Association, working under the leadership of Congressman Jared Polis, a Democrat from Colorado, and Congressman Luke Messer, a Republican from Indiana. The Pledge has now been signed by over 120 companies who have committed to use student data only for authorized educational purposes and not for things like targeting advertisements to students.

But more needs to be done. That includes working with schools to help educate them about how technology works and about the growing collection and use of data about students. That includes working with parent groups like the National PTA to help educate parents about the use of student data. And importantly, it includes passing laws to impose clear rules on the use of student data by technology companies.

But more needs to be done. That includes working with schools to help educate them about how technology works and about the growing collection and use of data about students. That includes working with parent groups like the National PTA to help educate parents about the use of student data.

---

<sup>21</sup> Senate Bill No. 1177, *available at*:

[http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill\\_id=201320140SB1177](http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177).

<sup>22</sup> This includes the following states: Arkansas, House Bill No. 1961, *available at*:

<http://www.arkleg.state.ar.us/assembly/2015/2015R/Acts/Act1196.pdf>; Delaware, Senate Bill No. 79, *available at*:

[http://legis.delaware.gov/LIS/lis148.nsf/vwLegislation/SB+79/\\$file/legis.html?open](http://legis.delaware.gov/LIS/lis148.nsf/vwLegislation/SB+79/$file/legis.html?open); Georgia, Senate Bill 89,

*available at*: <http://www.legis.ga.gov/Legislation/20152016/153829.pdf>; Maine, Legislative Document 454,

*available at*: <http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0183&item=3&snum=127>;

Maryland, House Bill No. 298, *available at*: <http://mgaleg.maryland.gov/2015RS/bills/hb/hb0298E.pdf>; New

Hampshire, House Bill No. 520, *available at*: <http://www.gencourt.state.nh.us/legislation/2015/HB0520.pdf>;

Oregon, Senate Bill No. 187, *available at*:

<https://olis.leg.state.or.us/liz/2015R1/Downloads/MeasureDocument/SB187/Enrolled>; Washington, Senate Bill

No. 5419, *available at*: [http://lawfilesext.leg.wa.gov/biennium/2015-](http://lawfilesext.leg.wa.gov/biennium/2015-16/Pdf/Bills/Senate%20Passed%20Legislature/5419.PL.pdf)

[16/Pdf/Bills/Senate%20Passed%20Legislature/5419.PL.pdf](http://lawfilesext.leg.wa.gov/biennium/2015-16/Pdf/Bills/Senate%20Passed%20Legislature/5419.PL.pdf).

<sup>23</sup> The Student Privacy Pledge, *available at*: [http://studentprivacypledge.org/?page\\_id=45](http://studentprivacypledge.org/?page_id=45).

Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052-6399

Tel 425 882 8080  
Fax 425 936 7329  
<http://www.microsoft.com/>



And importantly, it includes passing laws to impose clear rules on the use of student data by technology companies.

We would be happy to discuss this with you further and we look forward to working with you as your efforts progress. Thank you for your consideration.

Respectfully submitted,

Ryan P. Harkins  
Director, State Affairs and Public Policy  
Microsoft Corporation