From a Cloud Service Provider: The Importance of Keeping Your School's Data Safe

February 7, 2013 - by Guest Author

> Published by Getting Smart http://gettingsmart.com/cms/blog/2013/02/from-a-cloud-service-provider-the-importance-of-keeping-your-schools-data-safe/

By Guest Author Cameron Evans

 In this digital age, when devices and networks are increasingly connected to services in the cloud, the information stemming from those connections has grown exponentially.

This data presents a number of new opportunities to schools. The ability to monitor, leverage and manage data for the improved delivery of teaching and learning in order to personalize student education and save on infrastructure costs, has many schools looking to capitalize on cloud technology.

In K-12 teaching, schools are taking advantage of the opportunity to reduce barriers to sharing best practices, curriculum planning and collaboration. They also utilize data to better understand their students' strengths and areas for growth, helping to provide a more tailored learning experience.

An increasingly popular trend is the expansion of Massive Open Online Courses (MOOCs) in K-20 education, and as one can imagine, these courses expose significant amounts of student and teacher information to schools, as well as to the service providers who operate these courses. Schools are moving from being Receivers of student data to the role of Disclosers of student data.

This significant shift in role creates both opportunity and responsibility: protecting the privacy of students and faculty.

Just a few weeks ago, a group of educators met in Palo Alto to draft an initial framework seeking to protect the interests of students as online education continues to grow, calling the document "A Bill of Rights and Principles for Learning in the Digital Age." One component of that exercise is a statement on student privacy rights, which explains:

"Students have a right to know how data collected about their participation in the online system will be used by the organization and made available to others. The provider should offer clear explanations of the privacy implications of students' choices."

This effort is a much-needed initial step in exploring what data is collected today, how it gets used and with whom it gets shared.

Education advocate Sherman Dorn has highlighted the importance of transparency by the service provider, noting that different online course providers had radically different data privacy policies, including one that allowed virtually unlimited use of student data by the provider, including sharing it with third parties.

And in her Data Protection Day 2013 Op-Ed piece "Privacy, Emerging Technologies, and New Uses of Data", the U.S. Department of Education Chief Privacy Officer reiterated the need for institutions using new technologies to think carefully about data collection, use and sharing practices and to consider not just the existing legal framework, but also broader concepts of respect and fairness.

Safer Internet Day took place earlier this week, and its theme of 'online rights and responsibilities,' underscores that need to not overlook student privacy rights in an increasingly online world. As schools move to cloud services to replace IT tools that were once managed locally, they are placing large amounts of data into the hands of the cloud provider and increasingly relying on these providers to be a partner with them on a range of privacy compliance issues.

As highlighted by the Department of Education's Chief Privacy Officer, one of the most important pieces of federal legislation that K-12 administrators should be aware of as they move to the cloud is the Family Educational Rights and Privacy Act (FERPA).

Originally passed in 1974 in the dawn of the era of electronic records, FERPA provides students access to their education records and control over the disclosure of information in those records. FERPA prohibits the disclosure of information contained in student education records without consent from parents, or students age 18 or older, if they are enrolled in any post-secondary educational institution.

As technologies have evolved, from primitive electronic records to all-encompassing cloud computing services, the Department of Education has provided useful guidance

on how FERPA applies to student information transmitted across or stored in those systems. The Department's Cloud Computing whitepaper explains that schools must ensure their cloud providers are contractually bound to adhere to the same data use and redisclosure restrictions that FERPA imposes on the schools themselves.

These restrictions might not be welcomed by cloud providers who hope to make commercial uses of the data transmitted through or stored in their systems, including advertising or marketing purposes. In today's Big Data world, we know there are many companies with business models based on amassing customer data and using it for advertising or marketing. Clearly these models are in tension with student privacy rights protected by FERPA.

Schools also need to be cognizant of the Children's Online Privacy Protection Act (COPPA). COPPA applies to online services directed to children under 13 that collect, use, or disclose personal information and usually requires parental consent for such activities. Enforced by the Federal Trade Commission (FTC), their guidance regarding COPPA's application to the school setting reminds us that cloud providers who collect and use student information for commercial uses not directly related to the provision of the service, must obtain parental consent.

Parents in many school districts have rightly expressed concern with school efforts to deploy cloud services that make commercial uses of their students' data. These concerns highlight the need for service providers to clearly disclose commercial data collection and use practices and for schools to provide clear communication to parents of any such practices.

Even though we live in a digital age where more information is shared publicly online, the privacy rights of our students are too important for school leaders and cloud providers to ignore. And as noted by researcher Daniel Solove, studies of parent attitudes on student privacy find that parents have significant concerns that the privacy rights of their children are not being adequately protected.

School administrators, parents and students deserve full transparency about the data collection and use practices of their cloud providers, and that these practices are consistent with the existing legal and regulatory framework.

Microsoft takes its responsibility as a trusted data steward for our customers and academic institutions seriously. We have partnered with compliance experts in a number of industries subject to privacy related regulation, to ensure we have a shared understanding of those requirements and can help customers meet them. As a result of those partnerships, we are currently the only major cloud provider that contractually addresses both FERPA and HIPAA in cloud service offerings, including Office 365 for education.

As a trusted data steward for many customers, we respect privacy restrictions which our customers are bound by, and do not scan emails, data or documents our customers

store in the cloud, nor do we co-mingle that data with consumer services for the purpose of building analytics, data mining or advertising.

Given the fast-paced move to the cloud, we at Microsoft strive to better enable education institutions with the tools to protect the privacy of their students and faculty and their institutional data at a time when that protection is needed most.

Mr. Evans is national and chief technology officer of U.S. Education at Microsoft. You can connect with him via Twitter: @EDUCTO.