Making Sense of Student Data Privacy

BY BOB MOORE
RJM Strategies, LLC

Student Data Privacy – It's not often you can find an issue where policy makers, parents, school administrators, technology leaders (aka, CIOs), and vendors all agree that something needs to be done, if not exactly what. For all of the hand-wringing, scare tactics, and misinformation it can be difficult for CIOs to understand what they need to know and do in order to protect the privacy of students and their data. The purpose of this report is to provide a brief overview of student data privacy issues and to suggest some concrete steps that school leaders can take.

It's important to understand that the privacy of students and data collected about them is not a new issue. There are two Federal laws most often cited regarding privacy. Family Education Rights & Privacy Act (FERPA) and Children's Online Privacy Protection Act (COPPA) were enacted in 1974 and 1998 respectively. When the U.S. Department of Education (U.S. ED) enacted FERPA no one could have imagined how technology would change in the ensuing four decades. And while COPPA isn't nearly as old, the Federal Trade Commission (FTC) couldn't have foreseen state longitudinal data systems, cloud services or mobile apps. While the laws and compliance with them are important, in order to really understand the privacy issue you have to think beyond the laws.

There are three fundamental issues related to the privacy of student data. By understanding these, you can begin to see why they raise so many privacy concerns, as well as why this is a difficult issue to address.

1. **When and what kind of information** can an online service provider or other commercial entity request from a student?
2. **What kind of data** can an online service provider collect about a student as they are using the service?
3. **Who controls use of the data** and what can the service provider do with data about a student, whether it is data given to the service provider or collected by the service provider?

We've all had the experience of providing information about ourselves when signing-up for an online service. Items such as name, e-mail address, telephone number, date-of-birth, and area code are common. While we don't like to provide information that would allow a company to contact us, we generally give up the information freely because we want access to the free service. It seems a small price to pay, but what about children? How much personal information should they be asked to provide? Should parents have the right to be notified about such requests, let alone the right to opt-out? These are the types of issues that COPPA addresses. For students under 13 years of age, COPPA places requirements on parental notification and consent with regards to collection of data.

Another experience familiar to us all is loading a web site or an app and being recognized without being prompted to login. We like it when our search results are tailored to our own interests or that advertisements presented to us online are personalized just for us. We understand browser "cookies" and that online search engines, shopping sites, games, apps, and other services are collecting data about us and that they use that to better personalize our experience. Many people don't realize that some online service providers may be selling that data to others so that other service providers, for example, can target us with advertisements.

The Big Four Privacy Laws Affecting K12

FERPA: Regulates the release of personally identifiable information and education records, including parental rights regarding notification of the release of records, as well as the right to review, inspect, and amend such records.

COPPA: Pertains to web sites and online services that seek to collect information about or from students under 13 years of age. It specifies language that should be in the privacy policy of the service, as well as when the service must have parental consent to collect the information.

PPRA: Establishes requirements related to parental notification and opt-out option when collecting information from students that may be used for marketing purposes.

HIPPA: Includes both privacy and security requirements regarding health related information.

Adults, who accept these tracking practices as a small price to pay for a personalized experience, are often the same to cry foul when it comes to tracking student usage. Is it acceptable for an education game app to collect data about a student's performance, so that it can then sell data about the student to tutoring services, for example? Would it be acceptable if a provider of a free cloud-based file storage and sharing service mined, or scanned, the contents of files? Or how about a free e-mail service that collects data about keywords mentioned in student e-mail so it can target advertisements? While these examples would likely seem unsavory to most, there are times when tracking, or learning about, student use could be extremely beneficial to the student and their learning. The more an application can learn about a student and how they make decisions along a learning path, the more it can appropriately challenge the student and ensure that they are making progress. All of these examples describe practices that FERPA attempts to address.

As anyone can see, the issue of student data privacy in the age of the Internet, cloud services, and mobile apps is complex and very difficult to sort out. Beyond FERPA and COPPA, there are other Federal laws with privacy provisions that affect other data collection and use practices in K12. When taken together, FERPA, COPPA, Protection of Pupil Rights Amendment of 1978 (PPRA), and the privacy provisions in Health Insurance Portability & Accountability Act of 1996 (HIPPA) make for a daunting collection of laws that often can overlap making compliance even more difficult.

Fortunately, there are some excellent resources that can help the school leaders. The U.S. ED's Privacy Technical Assistance Center at http://ptac.ed.gov is one of the better resources for information about the application of key privacy laws affecting K12 schools. This is a must-know resource for school CIOs. The U.S. ED and FTC are quite active in updating interpretations and compliance guidance, so you need to stay current.

In March 2014, Consortium for School Networking (CoSN) released the Protecting Student Privacy in Connected Learning toolkit. It is a collection of practical, easy-to-digest resources that include a how-to flowchart for FERPA and COPPA, as well as suggested service provider contract terms, security questions to ask your online service provider and information about "click-wrap" agreements, data de-identification and other emerging privacy issues. CoSN's toolkit, which is free, was developed in cooperation with the Berkman Center for Internet & Society at Harvard University and the Harvard Cyberlaw Clinic. It has been endorsed by the Association of School Business Officials International. Microsoft provided underwriting support for the toolkit. CoSN plans updates and additions throughout the year. Go to http://www.cosn.org/focus-areas/leadership-vision/protecting-student-privacy to download the toolkit.

Unfortunately, there is no "easy button" for privacy issues. This is an issue where you have to study, research, network with others and just know that the more you work with it, the more understandable it will become. To make matters more challenging, the privacy landscape is changing constantly and if confusing Federal laws were not enough, more than 80 state statutes have been proposed in 2014 as of this writing. With that said, here is the Top 10 of my privacy to-do list for school leaders:

1 **Designate a Privacy Official** – Decide who in the district is responsible for privacy. You don't necessarily need to have someone with the Chief Privacy Officer title as some very large organizations increasingly do, but a senior administrator needs to be designated as the person responsible for ensuring accountability for privacy laws and policies. This is a "divide and conquer" issue, but someone needs to be in charge.

2 **Seek Legal Counsel** – All schools have access to the services of legal counsel for a variety of issues. Regardless of how your school is provided those services, make sure that you have access to counsel that understands the privacy laws and how they are applied to technology services. Do not wait until there is a pressing issue that needs to be addressed.

3 **Know the Laws** – As discussed already, this is not easy, but it is essential. In addition to U.S. ED and CoSN resources mentioned, many other organizations have developed or will be developing privacy-related materials. Don't forget about state laws or proposed state laws.

4 **Adopt School Community Norms & Policies** – It is generally accepted that laws such as FERPA and COPPA are the bare minimum when it comes to protecting privacy. There needs to be consensus among all stakeholders regarding collecting, using, and sharing student data. In doing so, ensure to balance the need for privacy with the desire for teachers to take advantage of innovative applications that may collect data to provide an adaptive, personalized experience. Without consensus on these issues it will be impossible to adopt enforceable policies.

Privacy Begins with Security

With all of the passionate discourse around privacy, it would be unfortunate if school technology leaders lost sight of perhaps the most fundamental aspect of privacy: security. It is often said that privacy is the objective of security. Stated another way, if data is not secure then you can't begin to assume privacy, regardless of how aggressively a district governs data collection, use, and ownership.

Security may not be easy, but there are generally accepted "smart practices" when it comes to security of devices, the data center, and network connections. Devices intended for consumer use, rather than institutional use, are generally less secure. Choose devices with security built-in. That's an important issue to consider when choosing a device and ecosystem for digital learning. CIOs sometimes struggle to get support for security measures and should not hesitate to use the issue of privacy as leverage.

As schools increasingly rely on online cloud services for learning, they may believe that they lose control of the security of their data. School technology leaders have the right and even the obligation to ask tough, specific security questions of online service providers. Any service provider that can't (or won't) answer your questions or agree to tough security language in a service agreement has not earned your school's business. Nothing less than complete transparency should be acceptable when it comes to security and privacy practices.

5 **Implement Workable Processes** – Bureaucracy is never desirable, but if your school is going to be serious about privacy there must be processes with checks and balances and accountability. No one wants to create roadblocks for innovation, but ensuring privacy requires some proactive planning and disciplined action on the part of school staff. Compliance with privacy laws suggest some very specific processes for schools. Once enacted, the processes should be reviewed regularly to ensure that they are workable and that they reflect current interpretations of the laws and of school policies.

6 **Leverage Procurement** – Every school RFP, bid, contract (or service agreement) has standard language around a wide range of legal issues such as indemnity, liability, payment and severability. By adopting standard language related to privacy and security you will make your task much easier. With that said, many online services are offered via "click-wrap" agreements that are "take it or leave it." If you are serious about privacy, you may have to ask staff to look for alternative solutions if the privacy provisions do not align with your expectations.

7 **Provide Training** – Schools are besieged with a never-ending list of professional development needs, but if you don't provide training for staff they will not know what to do or why it is important. Annual privacy training should be required of any school employee that is handling student data, adopting online education apps, and procuring and contracting with service providers. Privacy laws represent legal requirements that need to be taken seriously.

8 **Inform Parents** – Parents should be involved in the development of privacy norms and should provide policy input, but those parents will represent a small portion of the parent community. Just as schools provide significant information about online safety and appropriate use, they need to put significant effort into making sure that parents understand the measures taken to protect student privacy.

9 **Make Security a Priority** – The importance of security to ensure privacy cannot be overstated. Secure the device, the network, and the data center. Many devices that are intended for enterprise or institutional use have security built-in. Those intended for consumer use typically do not. Toughen password policies. Have regular security audits conducted by a third party expert. Make sure that RFPs, bids, and contracts have clear and enforceable security provisions for your online service providers.

10 **Review and Adjust** – Interpretations of privacy laws are changing and new laws may be added. School policies and practices will need updating and adjustment so that they reflect legal requirements. Processes can become burdensome and when that happens, some people may want to skirt the process. Seek input from those involved to ensure that the processes are not hindering teaching and learning.

The issue of privacy of student data is not going away. In fact, the more schools adopt online, cloud services for educational purposes, privacy issues will only become more pressing. By working to understand the concerns and the relevant laws, school leaders can begin taking concrete steps to better ensure the privacy of their students, while still encouraging the use of innovative technologies.

BOB MOORE

With more than 25 years in education technology, Bob Moore works with schools, education organizations, nonprofit associations, and business clients as a strategist, advisor, and subject matter expert. Bob started RJM Strategies, LLC following several years as lead strategist for a large global technology company and a career of two decades as a CIO in K-12 schools.

E-mail: BobMoore@RJMStrategies.com

Twitter: @BobMEdTech

LinkedIn: http://www.linkedin.com/pub/bob-moore/0/ba4/675/

Printed in USA 0514/SL/HBD/PDF ♻ Please Recycle