Privacy and school data

New technology “clouds” student data privacy

Just as technology delivers promising devices and applications to enhance learning, heightened privacy concerns call on schools and systems to become more involved and technology literate.

By Keith R. Krueger and Bob Moore

The issue of privacy has taken the education community by storm like no other since our organization, the Consortium for School Networking (CoSN), began serving school system technology leaders in 1992. Fueled by headlines about government security agencies reading emails and listening to phone calls of U.S. citizens, and by credit card data breaches at major retailers, student data privacy has become a priority for all stakeholders in the education community.

KEITH R. KRUEGER (keith@cosn.org) is chief executive officer of the Consortium for School Networking (CoSN), Washington, D.C. BOB MOORE (bobmoore@rjmstrategies.com) is founder of RJM Strategies, LLC and project director of CoSN’s Protecting Privacy in Connected Learning initiative.
This could not have come at a more unfortunate time for educators and students who are finally beginning to realize the tremendous value of a wide range of new, exciting education technologies. For years, teachers and education technology leaders talked about the promise of technology, but there were always obstacles to realizing the potential. Whether it was the lack of understanding of good professional development practices, digital content, bandwidth, low-quality mobile devices, or other obstacles, the promise of technology to enable and inspere teachers and students was typically far beyond what practically could be achieved.

Today, however, the increased commitment to professional development, access, digital content, and apps available for an array of high-quality, affordable mobile devices, the thirst for and use of technology for teaching and learning finally has gained significant momentum. School systems have invested considerable funding in technology tools and resources and in the human resources to integrate, operate, and maintain education technology. As a result, a new leadership role has emerged in school systems — that of the chief technology officer. These CTOs face a daunting challenge — along with those they serve — of pushing for the innovative use of technology by teachers and students while protecting student privacy and reassuring parents.

Evolving privacy issues

Student data privacy is hardly a new issue. Two of the most significant federal privacy laws affecting schools — the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA) — were enacted in 1974 and 1978, respectively. The web, as we know it today, did not emerge until two decades later. Even the one federal privacy law enacted in the Internet era, Children’s Online Privacy Protection Act (COPPA), took effect back in 2000 — long before smartphones, tablet computers, mobile apps, and cloud computing. As we’ve come to realize, privacy issues will evolve as the technology evolves.

Just as COPPA was taking effect, Congress passed the Children’s Internet Protection Act (CIPA) with the intent of shielding children from content that might be considered inappropriate for minors. When taken together, COPPA and CIPA created significant protections for a child’s online experience. Initially most schools treated these laws like a compliance box to check off. Yet as Internet use spread and grew beyond simple web sites to social networking and other types of online tools and communities, the challenge of providing a safe online experience for students required going far beyond compliance.

Not so helpful was the trend in many school systems to ban technologies in the name of safety, especially through restrictive, so-called Acceptable Use Policies. This lockdown-the-network approach to Internet safety often has created limited functionality of technology in schools and stifled innovative applications. Only in recent years have school systems moved from tightly restrictive policies that ban technologies to responsible use policies that focus on appropriate behavior.

We know that privacy will be an evolving issue as technology continues leaping forward. We must begin to consider steps that schools need to be taking (and realistically can take) to better address the privacy concerns of parents and policy makers while continuing to encourage the use of innovative new technologies and online tools for learning. Before we head down that path, let’s consider the actual privacy concerns, which may be very different depending on your perspective.

School data

Schools always have collected and used a variety of data. As long as that data is held within the school or school district, there are relatively few privacy concerns — unless, of course, there is a security breach. But this is where the emergence of new technologies such as cloud computing and software-as-a-service can create privacy issues. Many districts are choosing to have their student information system vendor operate the application in the cloud rather than remaining under the direct control of the school, which raises FERPA questions and concerns by the public. Similar concerns arise when schools upload data to online services that can run sophisticated analytics to see trends in student learning or program effectiveness.

School systems need data such as demographics, contact information, attendance, grades, health issues, accommodations information, and assessments. Most of these data are used only by authorized individuals in the school system. Sometimes the state education agency may need a small amount, and certain federal programs may require a very small amount. In either case the school system has direct control over the data and how they are used.

Value of school data

The focus on privacy concerns and compliance means the value of data is often overlooked. (See “The who, what, and why of school data” sidebar on page 21.) Also, consider the following data categories and their educational value:

- Contact and demographic data such as address, phone number, gender, and age — Used
Student data privacy has become a priority for all stakeholders in the education community.

THE WHO, WHAT, AND WHY OF SCHOOL DATA

WHAT’S COLLECTED

• General information: addresses, phone numbers, gender, age, physical or mental challenges;
• Local, state, and national assessments;
• Attendance, grades, participation in extracurricular activities;
• Surveys and other feedback.

WHO NEEDS IT AND WHY

TEACHERS
need data to understand when students are thriving and when they need more support in learning specific concepts.

PARENTS
and guardians need access to their child’s educational data to help them succeed.

STUDENTS
need feedback on their progress so they can make good decisions about program choices and prepare for success.

SCHOOL OFFICIALS
and community members need to understand school performance and know if scarce education resources are being allocated fairly and effectively.


for communication and improving school operations.
• Student attendance and grades — Used to show student progress.
• Test and assessment results — Used to highlight student progress and effectiveness of the education program.
• Preference and usage collected through surveys and feedback loop data on issues such as school facilities, learning climate, and diversity — Used to monitor and adjust school to better meet student needs.

There are two basic concerns with school data collected and held on the cloud. First, some worry about Big Brother; they contend that education should be entirely local, and that state and federal governments should have no interest in or access to local education data. Similar concerns were raised regarding inBloom Inc.’s effort to acquire massive amounts of private data about students in an effort to better coordinate and improve their school achievement. A firestorm of criticism brought that effort to a halt. The other concern relates to the security of the systems the data are stored on. With hacking (intentional, unauthorized access) of commercial data systems perceived to be commonplace, parents are concerned that even if data about their students are used appropriately, the data could be stolen, resulting in a serious privacy breach.

How online providers use data

As mentioned previously, data are not only important to education institutions. Web site operators as well as online service and app providers also may collect data. A common concern with this is often that these vendors will track a student online and then target advertising to the student or use data collected about the student in other ways to profit from the data. In 2014, states considered more than 100 bills dealing with privacy concerns, and many were targeted at commercial uses (Data Quality Campaign, 2014). In September 2014, California’s Student Online Personal Information Protection Act (SOPIPA) was signed into law and became the first comprehensive state legislation regulating the commercial collection and use of student data by online service providers. SOPIPA may be viewed as a model for student privacy legislation for other states to consider. It may seem obvious that such commercial uses of data collected about student online usage should not be allowed. On the other hand, the providers of free online services and apps are typically for-profit businesses and must generate revenue to pay employees and to add new features to their apps or services. Can “free” really be free?
The Protecting Privacy in Connected Learning toolkit can help school systems with the many intricate issues related to compliance with FERPA and COPPA when using an online service provider: www.cosn.org/privacy

CoSN developed this free, downloadable toolkit with the assistance of the Harvard University Cyberlaw Clinic and the Berkman Center for Internet & Society and sponsored by Microsoft, Lightspeed Systems and Schoolwires.

Most data collected by web sites, apps, or online services about a student’s use is employed legitimately. Most online shoppers value having their favorite shopping sites not only remember them but keep track of their purchases and even what they viewed. Online retail sites continue to refine and personalize the shopping experience so that it’s both more efficient and relevant for the shopper. The same can be true for online education services that track student usage and collect data about their preferences. They can turn that data into a much more personalized and relevant experience for the student. Since personalized learning is a high priority for parents and educators alike, we want to avoid passing laws that overreach and prevent online service providers from personalizing a student’s experience.

Online gaming is perhaps the best example of how an application or program can learn about a player and then adapt the game to the needs, interests, and tendencies of that player. That level of personalization and progressive challenges gives a glimpse of what could be done with online learning activities.

The debate over the strictness of privacy laws, what data should be collected by schools or service providers, who has access to that data, and how data can be used will continue to evolve as the technology evolves. But school systems can act now to take some very concrete steps to better ensure the privacy of student data. This list is adapted from www.k12blueprint.com/content/10-privacy-steps-every-district-can-take-today.

Step #1. Designate a privacy official.

Just as school systems typically have a senior administrator who is accountable for compliance and other important issues, school districts should designate a senior administrator who is responsible for ensuring accountability for privacy laws and policies. This is not necessarily the chief technology officer or system technology leader. The scope of the privacy issue is beyond any one individual, but knowing where the buck stops is critical.
Most data collected by web sites, apps, or online services about a student’s use is employed legitimately.

**Step #2. Engage legal counsel.**
Ensure that your school district has access to legal counsel who has expertise in privacy laws and how those laws apply to education technology services. This is instrumental in helping you understand your compliance obligations and developing school policies and practices. Don’t wait until there is a pressing issue that needs to be addressed. Privacy issues that have made headlines in recent months tell us that this issue takes on extreme urgency when there are concerns.

**Step #3. Get to know the laws.**
Remember that several federal laws apply to student data privacy. Three have been mentioned previously in this article: COPPA, FERPA, and PPRA. The Health Insurance Portability & Accountability Act (HIPAA) also has privacy provisions that may apply to some of your student records. And with more than 100 state statues proposed in 2014 and many more anticipated for the 2015 legislative session, if your state has not passed new student data privacy legislation, it likely will. Many organizations have and will be publishing privacy guidance for schools, such as the CoSN toolkit mentioned earlier. The U.S. Department of Education’s Privacy Technical Assistance Center is a must-know resource at http://ptac.ed.gov/.

**Step #4. Adopt school community norms and policies.**
As noted already, it would be easy to view privacy as a mere compliance issue to check off, but we have already seen that mere compliance with long-standing federal laws is insufficient. It is important to have a dialogue about and reach consensus on issues such as what data is collected, how it is used, who has access to it, and community tolerance for online service providers collecting and using student data.

**Step #5. Implement workable processes.**
Some school systems have very centralized decision making, and others allow individual schools and even classroom teachers a great deal of latitude in deciding things such as instructional content and applications. In all cases, systems should have processes for selecting instructional apps and online services that ensure data privacy is considered. Teachers may be capable of determining the educational value of an app, but even the savviest privacy experts often find it impossible to determine what data an app collects and what is done with the data. No one wants to slow innovation, but ensuring privacy requires some planning and adherence to processes. Never forget that failing to comply with applicable federal and state laws because they aren’t convenient is no excuse. Once enacted, the processes should be reviewed regularly to ensure they’re workable and reflect current interpretations of privacy laws and policies.

**Step #6. Leverage procurement.**
Every bid or contract has standard language around a wide range of legal issues, such as liability, termination, and payment. Adopting standard language related to privacy and security will make the task much easier. The CoSN toolkit has suggested contract terms that should be helpful. Unfortunately, many online services are offered via “click-wrap” agreements that are “take it or leave it.” You may have to look for alternative solutions if the privacy provisions of those services don’t align with your expectations. This is yet another reason to have established processes to select and adopt cloud-based and online services as well as mobile apps.
Failing to comply with applicable federal and state laws because they aren’t convenient is no excuse.

Step #8. Involve parents.

The privacy of student data is increasingly a red-flag issue for parents. Parents should be involved in developing privacy norms and policies. Just as schools provide information about online safety and appropriate use, they need to put significant effort into ensuring that parents understand the measures taken to protect student privacy, as well as the educational value of data. All federal privacy laws have some form of parental rights provisions.

Step #9. Data security must be a priority.

Privacy starts with security. Employees in school systems often push back against security measures because they can seem confining. You have to find a balance, but protecting the security of data should be an absolute priority. Secure the device, the network, and the data center. Toughen password policies. Have a third-party expert do regular security audits. Insist that your online service providers have robust security practices.

Step #10. Monitor and adjust.

Just as teachers monitor student progress and adjust instruction accordingly, school system leaders must monitor privacy processes and practices to ensure that they are working for all interests in the school system. In addition, interpretations of privacy laws are changing and new laws may be added. School policies and practices will need updating so they reflect current legal requirements. Processes can become burdensome and when that happens, some people may want to skirt the process. Ensuring that doesn’t happen is essential.

Step #7. Insist on professional development.

All staff involved with selecting and adopting apps and online services must have regular training on privacy issues. This is no different than other compliance issues that are often considered required training each year in most school systems. This also applies to any school employee handling student data and contracting with service providers. Privacy laws represent legal requirements that need to be taken seriously.

Conclusion

Privacy concerns raised by parents, policy makers, and privacy advocates are very real. Some would want us to believe that the concerns are overstated. The fact is that there is a very specific body of federal laws that address the privacy of students in K-12 school systems. State legislatures are considering unprecedented restrictions on the collection and use of student data. Just as the laws and the technology they govern will evolve, so too should the practices of school systems.

Reference
