HOUSE EDUCATION AND THE WORKFORCE COMMITTEE
SUBCOMMITTEE ON EARLY CHILDHOOD, ELEMENTARY AND SECONDARY EDUCATION

“HOW EMERGING TECHNOLOGY AFFECTS STUDENT PRIVACY”
FEBRUARY 12, 2015

TESTIMONY OF SHERYL ABSHIRE
CHIEF TECHNOLOGY OFFICER
CALCASIEU PARISH PUBLIC SCHOOLS
LAKE CHARLES, LOUSIANA

Introduction

Thank you, Chairman Rokita, Ranking Member Fudge, and members of the subcommittee, for inviting me to testify about technology’s impact on student privacy and confidentiality. For over 40 years, I have served Louisiana Public Schools as a teacher, school librarian, principal, and technology leader. I now serve as the Chief Technology Officer of the Calcasieu Parish Public Schools in Lake Charles, Louisiana, and I am also a member of the Board of Directors for the Consortium for School Networking (CoSN), a national professional organization for school district technology leaders.

Framing the Issue

I appreciate this opportunity to discuss how our district uses technology to support teaching and learning and to share our strategy for balancing effective technology and data use with strong student data privacy protections. Technology and data use play a central role in our district’s strategy for supporting teaching and learning, as well as in improving the system’s planning, evaluation, and continual improvement. Equipped with the right technology, high quality professional development, and appropriate data, our teachers can tailor and individualize instruction, engage students, and deliver rich digital resources. Our district also equips parents and guardians with the data they need to monitor, understand and support their children’s educational progress; grants school and district leaders with data to identify and address program performance gaps and make better management decisions; and provides state leaders with aggregate data to better assess the effectiveness of important state college and career readiness education reforms. Finally, we are on the cusp of providing real-time data to our students to enable feedback that deepens their learning and helps them go deeper, learn faster, and understand areas needing improvement.

Using technology to provide the right people, with the right data, at the right time is critical to effective decision-making at the classroom, school, district and state levels. We believe robust data sharing, however, must be complemented by well-designed strategies and practices to protect student privacy and ensure confidentiality. In our district, these protections include equipping our schools with well-designed privacy policies; ensuring implementation of technical, physical and administrative safeguards; and strengthening our educator, school leader and staff capacity to effectively use and protect personally identifiable data. We also take steps to continually educate our parents and other stakeholder groups about our district’s technology, data use, and privacy strategies, so that the “what, where, and when” of our practices are understood and broadly supported by the community.

District Vision and Practice

Our district has taken an aggressive and comprehensive approach to assuring student privacy. We have created extensive data sharing training materials and all employees in the district, from the school custodians, bus drivers, to teachers and principals, have participated in the training sessions outlining the permissible uses of student data sharing. Upon completion of the required training, each year, every district employee signs a statement of assurances to acknowledge their understanding and compliance with student data sharing polices and laws of the district and state. This process is based on the CoSN Protecting Privacy in Connected Learning Toolkit produced in partnership with Harvard Law School's Cyberlaw Clinic and is free to all school systems.

Calcasieu Parish Schools strongly emphasize both appropriate technology and secure and safe data use, including using data to develop a greater understanding of student needs and then tailoring instruction and delivery of resources to help them succeed. Over the past three years, our district developed a leading-edge data warehouse and data dashboard to provide our teachers and school leaders with the timely, targeted information they need to support learning. Our system provides every school leaders and teachers in the Calcasieu Parish Schools with rich diagnostic information – including formative and summative results and other indicators – about each learner and their progress toward achieving Louisiana's college and career ready standards. This monitoring enables us to keep students on track for graduation, including identifying warning signs that might signal serious problems such as a greater likelihood to fall behind grade level or drop out. Based on my experiences in Calcasieu Parish, I urge Congress to proceed cautiously with new federal privacy requirements. We want to be sure that any contemplated legislation does not impede this type of powerful instructional data use.

Community-based organizations, researchers and private partners play an important role in supporting our district's efforts to meet the needs of every student. Collaborating with partners, including appropriately and lawfully sharing student information with them to improve teaching and learning, and to support school and district decision-making, greatly enhances our ability to improve student outcomes and efficiently run our district. For example, we work with all of our vendor partners that use any student data as part of a learning or assessment system. We require them to certify their compliance with our data usage policy. Our state law reasonably addresses such sharing by requiring all vendors to sign contracts securing their commitment to protect student data, specifying the limited purposes for which the student information may be used, and, as required by FERPA, ensuring that sensitive data always remains under the control of the district. CoSN's Security Questions to Ask of an Online Service Provider has been helpful in identifying the key elements we expect of companies.

Congress must carefully avoid overreaching in ways that might create unintended consequences for educationally appropriate data sharing, including avoiding legal prescriptions that disrupt suitable private partnerships, research, evaluation and other activities designed to support district administration and related policymaking or stifle the use of innovative and effective web-based technology resources.

Our district prioritizes teacher and school leader staff development. We believe successful data use, including ensuring best in class privacy protections, not only requires sounds policies and practices, but also meaningful attention to building the capacity of our school leaders, teachers and other staff. Teachers and school leaders must be equipped with the right technology and the knowledge about how to use and protect student data with fidelity to implement best practices. As a result, we support successful implementation of our data systems and practices with regularly targeted professional development designed to equip our educators and school leaders with the knowledge they need to use data to improve student outcomes, including training them in privacy and security best practices. Additional federal investments in technology and student privacy focused professional development, including through the Enhancing Education through Technology Program, would contribute significantly to helping districts protect student data privacy by ensuring they have access to leading-edge security protections and equipping education professionals with the knowledge they need to successfully implement privacy policies and protocols. I encourage Congress to support the President's FY 2016 request to fund this important program. Unfortunately this program has not received funding since 2011.

Our district prioritizes communicating with stakeholders to convey the value of data to teaching, learning, and decision-making. With this goal in mind, we work to ensure that our parents and communities find value in the data that is collected and understand the "who, what, where, and when" of data collection and use. We also established a clearly understandable data inventory and description of the data we use. All of this information is made readily available to our parents and community on our district webpage. This step not only builds trust and understanding in our community, but also forces our district to reflect on our data use practices and ensure that we are not unnecessarily collecting student information. Informed communities become allies in both effective data use and privacy protection and recruiting them begins with efforts to promote transparency. CoSN and the National School Public Relations Association have produced a helpful infographic which school districts can use with their parents / guardians to convey why we collect data and how we protect it. This type of transparency is key to building trust with our communities. Congress should consider strategies that encourage districts to promote data use transparency, including describing the "who, what, where, and when" of their technology and data practices.

Finally, our district strives to routinely review and update our privacy, technology and data use policies, so that they reflect our educational needs and evolving privacy best practices. Protecting student data is not a one-time event. Educators' data needs evolve, security threats are constantly changing, and professional development needs are ongoing. We work to ensure that our policies reflect this dynamic environment so that we can meet our professional's needs and anticipate and address policy or practice gaps that might compromise the privacy of our students. Congress should encourage districts to implement security practices that meet mature technical, physical and administrative standards. Congress should also encourage districts to continually examine and update their privacy and security policies and practices and provide the resources needed to ensure our schools remain on the leading edge of privacy protections.

Conclusion

While federal and state privacy policy is critically important, school districts and schools must lead efforts to protect student data privacy. Any effort by Congress to update federal privacy laws to better protect students, including improvements to FERPA and Children's Online Privacy Protect Act (COPPA), should support, not burden school, district and state data use to improve instruction and decision making. Appropriate data sharing with researchers, evaluators and private partners engaged in supporting educational and administrative activities must be preserved to strengthen the potential of technology to transform and improve education.

Although they have some weaknesses, FERPA and COPPA already provide a strong foundation for local privacy leadership and decision-making. Any new federal law should concentrate on addressing clear gaps in the present system, including the absence of a focus on ensuring technical, physical and administrative protocols and especially the lack of sufficient resources for professional development targeting educators, school leaders and staff.

I urge Congress not to overreach as it addresses this important issue, but instead to take a thoughtful, balanced approach focused on supporting district and school leadership.

I thank the members of the Committee for the opportunity to share a realistic view of this issue from the perspective of a school district. I will be happy to answer any questions the Committee might have.

ADDENDUM

CoSN's *Protecting Privacy in Connected Learning Initiative*

This CoSN-led effort provides school leaders and stakeholders with a suite of resources to help them navigate the four major federal privacy laws and address key questions about protecting student privacy.

The resources offered through the initiative include an in-depth, step-by-step toolkit; infographics to empower schools leaders to clearly discuss the issue; and additional complementary, standalone tools.

The resources can be downloaded for free at: cosn.org/privacy.

Ten Steps Every District Should Take Today

With so much uncertainty about what districts can or should be doing to help ensure the privacy of student data, it would be easy to lose sight of some very concrete steps that can be taken today.

1. **Designate a Privacy Official**—A senior district 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**—Make sure that the legal counsel your district has access to understands education 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**—Many organizations have and will be publishing privacy guidance for schools, such as the toolkit CoSN toolkit available at http://www.cosn.org/privacy. The US Department of Education's Privacy Technical Assistance Center is a must-know resource at http://ptac.ed.gov/.

4. **Adopt School Community Norms & Policies**—Beyond the privacy laws, what does the school community really expect when it comes to privacy? Seek consensus regarding collecting, using and sharing student data.

5. **Implement Workable Processes**—There must processes for selecting instructional apps and online services. No one wants to slow innovation, but ensuring privacy requires some planning and adherence to processes. Once enacted, the processes should be reviewed regularly to ensure that they are workable and that they reflect current interpretations of privacy laws and policies.

6. **Leverage Procurement**—Every bid or contract has standard language around a wide range of legal issues. By adopting standard language related to privacy and security you will make your task much easier. Unfortunately, many online services are offered via "click-wrap" agreements that are "take it or leave it." You may have to look for alternatives solutions if the privacy provisions of those services do not align with your expectations.

7. **Provide Training**—Staff need training so they will know what to do or why it is important. Annual training should be required of any school employee that is handling student data, adopting online education apps 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 policies. Just as schools provide 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**—Privacy starts with security. Secure the device, the network and the data center. Toughen password policies. Have regular security audits conducted by a third party expert.

10. **Review and Adjust**—Interpretations of privacy laws are changing and new laws may be added. School policies and practices will need updating and adjusted so that they reflect legal requirements. Processes can become burdensomand when that happens, some people may want to skirt the process.

Excerpted from Making Sense of Student Data Privacy (May 2014), authored by Bob Moore, Founder, RJM Strategies LLC and supported by Intel. The full report can be found at http://www.k12blueprint.com/privacy.

Our Commitment to You: CLEAR PRIVACY PRACTICES

Parents and guardians want assurances that personal information and data about their children are secure and protected by our school system. These questions are rising as we use the Internet, mobile apps, cloud computing, online learning and new technologies to deliver exciting new education services.

At our school we strive to be clear about what data we collect, how data supports your child's education and the safeguards in place to protect that data.

What Data do We Collect and Why?

School Operations

We collect data such as addresses and phone numbers, gender and age, as well as information to ensure student safety, and accurate reporting to help run our school operations efficiently.

Measuring Progress and Participation of our Students

We collect data such as attendance, grades and participation in school-sponsored extra-curricular activities to enable students to succeed.

Improving the Education Program

We collect results from local, state and national assessments to provide teachers, administrators and parents important information about student, program and school performance and improve the education programs we offer.

Striving to Meet the Needs of Students

We collect surveys and other feedback to improve teaching and learning and address other issues important to students and their families.

How Education Data Supports Student Success and School Improvement

data=success!

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.

How is Education Data Protected?

We follow federal and state education privacy laws and adhere to privacy and security policies.

» For example, the Family Education Rights & Privacy Act (FERPA) gives parents rights related to their children's education records and personally identifiable information. Additional information is available in our annual notice to parents of their rights under FERPA and from the U.S. Department of Education at http://familypolicy.ed.gov/.

When we use an online service provider to process or store data, they also must adhere to certain federal and state and privacy laws. We also expect them to use current security protocols and technology.

» Additionally, the federal Children's Online Privacy Protection Act (COPPA) prevents child-directed websites and apps from collecting certain personal information from anyone under 13 years of age without parental permission. Our school system may consent on behalf of parents in the education context when student information is collected for the school's exclusive use and benefit and for no other commercial purpose.

» Under FERPA, our vendors cannot use the education records we provide in any way that is not authorized by the school district. They cannot sell this data or allow others to access it except as we permit in accordance with federal and state education privacy laws.

Our Commitment

We are working to improve your children's education by ensuring it meets their unique needs. It would be very difficult to accomplish this goal without the ability to capture important information about your child's progress. Protecting personal information in secure and responsible ways is at the heart of our efforts to provide a richer and more dynamic learning experience for all students.

LEARN MORE about the rights of parents and guardians at **dataqualitycampaign.org/pta** or **PTA.org/Parents** or **commonsensemedia.org**

Security Questions to Ask of An Online Service Provider

It is important to understand your provider's security practices to ensure that data shared with and collected by the provider remain private and protected. You should work with your School System's security point of contact to determine whether the security practices of the provider comply both with School System policies and applicable laws. While neither FERPA nor COPPA prescribes specific security standards, school systems should look to industry suggested practices when assessing an online service provider.

The following is a non-exhaustive list of key security questions to discuss with your provider. A service level agreement (SLA) should include as many of these considerations as possible.

Data Collection

- What data does the provider collect?
- What, if any, data is collected by 3rd parties (e.g., via cookies, plug-ins, ad networks, web beacons etc.)?

Network Operations Center Management and Security

- Does the provider perform regular penetration testing, vulnerability management, and intrusion prevention?
- Are all network devices located in secure facilities and under controlled circumstances (e.g. ID cards, entry logs)?
- Are backups performed and tested regularly and stored off-site?
- How are these backups secured? Disposed of?
- Are software vulnerabilities patched routinely or automatically on all servers?

Data Storage and Data Access

- Where will the information be stored and how is data "at rest" protected (i.e. data in the data center)?
    - Will any data be stored outside the United States?
    - Is all or some data at rest encrypted (e.g. just passwords, passwords and sensitive data, all data) and what encryption method is used?
- How will the information be stored? If the cloud application is multi-tenant (several districts on one server/instance) hosting, how is data and access separated from other customers?
    - FERPA requires that records for a school be maintained separately, and not be mingled with data from other school systems or users.
- Are the physical server(s) in a secured, locked and monitored environment to prevent unauthorized entry and/or theft?
- How does the provider protect data in transit? e.g. SSL, hashing?
- Who has access to information stored or processed by the provider?
    - Under FERPA, individuals employed by the provider may only access school records when necessary to provide the service to the School System.
    - Does the provider perform background checks on personnel with administrative access to servers, applications and customer data?
    - Does the provider subcontract any functions, such as analytics?
    - What is the provider's process for authenticating callers and resetting access controls, as well as establishing and deleting accounts?
- If student or other sensitive data is transferred/uploaded to the provider, are all uploads via SFTP or HTPPS?

Data and Metadata Retention

- How does the provider assure the proper management and disposal of data?
  - The provider should only keep data as long as necessary to perform the services to the School.
- How will the provider delete data?
  - Is data deleted on a specific schedule or only on termination of contract? Can your School request that information be deleted? What is the protocol for such a request?
- You should be able to request a copy of the information maintained by the provider at any time.
- All data disclosed to the provider or collected by the provider must be disposed of by reasonable means to protect against unauthorized access or use.
- Upon termination of the contract, the provider should return all records or data and properly delete any copies still in its possession.

Development and Change Management Process

- Does the provider follow standardized and documented procedures for coding, configuration management, patch installation, and change management for all servers involved in delivery of contracted services?
- Are practices regularly audited?
- Does the provider notify the School System about any changes that will affect the security, storage, usage, or disposal of any information received or collected directly from the School?

Availability

- Does the provider offer a guaranteed service level?
- What is the backup-and-restore process in case of a disaster?
- What is the provider's protection against denial-of-service attack?

Audits and Standards

- Does the provider provide the School System the ability to audit the security and privacy of records?
- Have the provider's security operations been reviewed or audited by an outside group?
- Does the provider comply with a security standard such as the International Organization for Standardization (ISO), the Payment Card Industry Data Security Standards (PCI DSS)?

Test and Development Environments

- Will "live" student data be used in non-production (e.g. test or development, training) environment?
- Are these environments secure to the same standard as production data?

Data Breach, Incident Investigation and Response

- What happens if your online service provider has a data breach?
- Do you have the ability to perform security incident investigations or e-discovery? If not, will the provider assist you? For example, does the provider log end user, administrative and maintenance activity and are these logs available to the School System for incident investigation?

Suggested Contract Terms

After your School System chooses an online service provider, it is important to draft a contract that specifies how the provider will comply with your School System's security requirements. Drafting a contract should be done under the guidance of your School System's legal counsel; however, the following suggested contractual terms identify key components to consider including.

The contract should specify the services to be provided and the provider's obligations, including the following:

1. **Contract Scope**. Identify all elements that comprise the agreement and what order of precedence is followed in the event of a contradiction in terms. Identify any contract terms that are incorporated by reference (e.g. URL).

2. **Purpose.** If you have determined that the provider qualifies as a "school official" under FERPA and you will use the school officials exception as the vehicle for disclosing FERPA protected information to a provider, specify: (i) that the provider is considered a school official, (ii) the legitimate educational interest that the provider is fulfilling, (iii) the nature of the data collected, and (iv) the purpose for which any FERPA protected information is being disclosed.

3. **Data Collection, Use and Transmission.** Specify how the provider may use or collect data from the School System and your students, and any restrictions that may apply to the provider's use of that data and ensure that you bind the provider to those uses and restrictions. At a minimum, you should address the following:

    - Specify that the provider should only be permitted to use any information stored, processed, or collected as necessary to perform the services for the School System. Include a specific restriction on the use of student information by the provider for advertising or marketing purposes, or the sale or disclosure of student information by providers.

    - Specify any metadata the provider will collect (e.g. logs, cookies, web beacons, etc.).

    - Specify any data and metadata any 3rd party will collect (e.g. analytics, etc.) as a function of the use of the provider's service.

    - Specify that the provider should be restricted from accessing, collecting, storing, processing or using any school records, and student or parent information, for any reason other than as necessary to provide the contracted services to your School.

    - Specify when and how the provider may disclose information it maintains to other third parties. Under FERPA, providers may not disclose education records provided by your School System to third parties unless specified in your contract.

    - Specify whether the School System and/or parents (or eligible students) will be permitted to access the data (and if so, which data) and explain the process for obtaining access. Consider if the contract needs to specify whose responsibility it is (the provider or the School System) to obtain parental consent and facilitate parent's request to access student educational records.

- Specify that data collected belongs to the School System (and/or its users) and that the provider acquires no rights or licenses to use the data for purposes other than for the delivery of the service.
- Specify that a provider must disclose if it will de-identify any of the FERPA protected data that it will have access to and if so, require that the provider supply details of its de-identification process. When appropriate, you may want to retain rights to approve such a process prior to the provider using or sharing de-identified data in ways that are beyond the purpose for which any FERPA protected information is disclosed.

4. **Data Security.** Specify any security requirements that the provider must follow to the extent that it maintains, processes, or stores any information on behalf of the School System. At a minimum, the contract should address the following:
   - The provider must securely maintain all records or data either received from the School System or collected directly from the school, teachers, students, or parents in accordance with the security standards designated by the School.
   - Information, content and other data collected and stored from and on behalf of the School System and the students should be stored and maintained separately from the information of any other customer, school, or user.
   - The provider should restrict access to your School System's information to only those individuals that need to access the data in order for the provider to perform the agreed-upon services.
   - The agreement should identify what happens if the provider has a data breach. The agreement should identify the provider's responsibilities including the School System's point of contact, required notification time, and any obligations for end user notification and mitigation.
   - You should have the right to audit the security and privacy of your School System's or students' records or data.
   - Require the provider to notify you in writing about any changes that will affect the availability, security, storage, usage or disposal of any information.
5. **Data Retention and Disposal.** Assure the proper management and disposal of data or information pertaining to the School or its students. All data disclosed to the provider, or collected by the provider, must be disposed of by secure means to ensure that it is protected from unauthorized access or use.

6. **Bankruptcy or Acquisition.** Specify what happens to the data if the provider goes out of business or is acquired by another firm. Is there a source code or data escrow provision?

7. **Service Levels and Support**.
   - Specify the service levels the provider must meet and any credits you receive for any failure by the provider to meet these service levels.
   - Require the provider to supply the School with all the technical assistance you may need to use the services.

8. **Governing law and jurisdiction.** Typically a provider's default contract will specify that it is governed by the law of the provider's home state. Public institutions generally have significant restrictions on their ability to consent to such provisions under the School System's local state laws.

   - Check with your legal counsel about what law can govern contracts entered into by your School in light of your School's state laws.

9. **Modification, Duration, and Termination Provisions.** Establish how long the agreement will be in force, what the procedures will be for modifying the terms of the agreement (mutual written consent to any changes is a best practice), and what both parties' responsibilities will be upon termination of the agreement, particularly regarding disposition of student information maintained by the provider. Upon termination of the contract, the provider should return all records or data and properly delete any copies still in its possession, including archives and/or backups.

10. **Liability**. The provider should be liable for the activities of its staff and subcontractors.

   - The provider should generally have an obligation to comply with all applicable laws, including privacy laws.
   - If the provider will be collecting data from children under the age of 13, the provider should comply with COPPA.
   - The provider should be liable for any breaches in security or unauthorized third party access arising out of the provider's breach of its contract obligations.
   - The provider should be liable to the School System for any claims or damages that arise as a result of the provider's failure to comply with its obligations as a Cloud Service Provider under COPPA, FERPA, or other applicable laws.
   - Limits of liability should be consistent with market-tested commercial practices and should appropriately allocate risk between the Vendor as a Cloud Service Provider and the Customer as the owner of its Data.
   - The School System may wish to identify through negotiation specific categories of direct damages that would be excluded from traditional definitions of consequential damages.

*Endorsed by **The Association of School Business Officials International**.*

COSN

LEADING EDUCATION INNOVATION

COSN.ORG/PRIVACY