BACKGROUNDER:
EDUCATION TECHNOLOGY: FRIEND OR FOE

Education technology facilitates personalized learning and allows educators to better target instruction based on identified needs. Technology also improves the ability of education researchers to evaluate instructional approaches and interventions and provides policymakers information to aid in decision making.

A majority of parents support the use of new technology and do not cite data privacy as a top tier education concern (compared to such issues as teacher effectiveness, standardized testing and school performance). Furthermore, data breaches in education are relatively uncommon.[1]

Nevertheless, several high profile incidents raised awareness of the amount of data being collected and the vulnerabilities where data are not properly secured.

For example:

- A school district in Pennsylvania failed to disclose that it installed tracking software on laptops issued to students, which was used to spy on students in their homes.[2]
- A third party contractor in Virginia inadvertently uploaded and left unprotected student directory information.[3]
- Chicago student information was accidentally posted online.[4]
- Health care provider chains inappropriately gained access to student information in Arizona and Tennessee and used the information to market services to parents.[5]
- Although there was no data breach, parents raised sufficient concerns about the storage of their children's educational records with a third-party repository that several school districts discontinued their participation with inBloom, a nonprofit funded by the Gates and Carnegie Foundations to provide a secure technology platform to monitor student performance.

Statutory protection has not kept pace with technology

The **Family Educational Rights and Privacy Act (FERPA)** limits the circumstances under which a school, district, or state education agency (SEA) may disclose personally identifiable information (PII)[6], and requires schools to inform parents of their right to review and correct their children's records. It also empowers parents to opt out of disclosure of information for purposes not specifically authorized by the law. FERPA does not require parental notification or consent for disclosure of educational records to contractors, consultants, and others over whom the educational institution exercises control.

NEA Education Policy and Practice Department
Center for Great Public Schools 1201 16th St., NW, Washington, D.C. 20036

20422.6/16.cdk

Those conducting education research, developing or evaluating assessments, or administering student aid programs may also be granted access, provided PII is not disclosed to anyone beyond representatives of the organization, and such information is destroyed when no longer needed.

- FERPA does not protect data that have been de-identified, or that fall within the exception of directory information. The law also contains law enforcement, and health and safety exceptions.
- FERPA also lacks any requirement that schools or other entities with access to education records adopt security procedures, or provide notification in the event of a security breach.
- Data that record information such as how long students take to perform assignments, or the number of attempts made may be stripped of PII, in which case FERPA does not prohibit its disclosure or use to develop or improve products and services.

The **Protection of Pupil Rights Amendment (PPRA)** requires school districts to work with parents to develop policies regarding the collection, use, and disclosure of personal information, including the district's privacy protection practices. PPRA also requires districts to allow parents to opt their children out of activities in which data will be collected, disclosed, or used for marketing purposes. PPRA does not apply to information collected for the exclusive purpose of developing, evaluating, or providing educational products or services for or to students or educational institutions.

The **Children's Online Privacy Protection Act (COPPA),** administered by the Federal Trade Commission (FTC), requires commercial Web site operators, online services, and technology apps that target children to obtain verifiable parental consent before collecting a child's PII. However, consent may be provided by a teacher or school where use of the site or service occurs at the direction of the school or teacher, the use is educational, and the data are not used for any commercial purpose beyond education.

The **Every Student Succeeds Act (ESSA)** maintains protections that were included in its predecessor, No Child Left Behind, and adds specific privacy protections, including a requirement that grant recipients understand their responsibilities under FERPA, and the prohibition against creation of a national database of PII. Also, Title II grant funds may be used to support training in the appropriate use of student data to ensure compliance with FERPA and any applicable state and local privacy laws and policies.

State legislative approaches include outright prohibitions against the collection of certain types of data, restrictions on the use of data, and data protection requirements. In 2015, more than 100 such bills were introduced across the country.[7] Enacting legislation without careful deliberation, however, can produce unintended consequences. For example, requiring schools to destroy student records after the student leaves the school would eliminate the ability to provide transcripts for graduates or records for students who change schools. Likewise, requiring prior consent for disclosure of any data to a third party, including researchers, could skew the data and impact findings. Prohibiting outsourcing data security and storage to a third party could impose virtually insurmountable challenges to school districts, many of which lack the internal capacity and expertise to bring this function in house.

Continued on page 3

GUIDANCE AND BEST PRACTICES

Certain themes run through the guidance and policy recommendations that the technology industry, privacy advocates, and education organizations have issued related to student data privacy. They include the following:

- Schools districts should develop, in collaboration with parents and educators, policies related to the collection, use, and safeguarding of student data, and procedures for responding to data breaches, and designate the office or individual responsible for compliance.
- Educational institutions should maintain control of student data and grant access only to those with legitimate educational needs.
- Education institutions should be transparent regarding the types of data being collected, the purpose for which it is being used, and with whom data are shared and for what purpose.
- Those with access to student data should have clear guidelines and training regarding collection, use, and security procedures.
- Data mining for advertising and marketing purposes should be expressly prohibited.
- Data security procedures and practices should be reviewed regularly.

The U.S. Department of Education's Privacy Technical Assistance Center (PTAC) also recommends that schools and districts negotiate privacy and security provisions of major contracts with education service providers, and review for privacy considerations Terms of Service (TOS), acceptance of which is often required as a condition of using a particular technology application.

Additional Resources

FERPA: A Legal Overview, Congressional Research Service
https://fpf.org/wp-content/uploads/2016/03/CRS_FERPAOverview_2013_11_19.pdf

Student Privacy Resource Center, a project of the Future of Privacy Forum
https://ferpasherpa.org/

Student Data Principles
Ten Foundational Principles for Using and Safeguarding Students' Personal Information developed and endorsed by a coalition of organizations, including NEA
http://studentdataprinciples.org/wp-content/uploads/2015/03/Student-Data-Principles-FINAL.pdf

Education Data Principles
National Association of State Boards of Education
http://www.nasbe.org/project/education-data-privacy/nasbepepdata

The Protecting Privacy in Connected Learning toolkit, The Consortium for School Networking (CoSN)
http://cosn.org/focus-areas/leadership-vision/protecting-privacy

Best Practices for the Safeguarding of Student Information Privacy and Security for Providers of School Services, Software & Information Industry Association
http://www.siia.net/Portals/0/pdf/siia_best_practices_for_student_info_privacy.pdf

K-12 School Service Provider Pledge to Safeguard Student Privacy, Future of Privacy Forum and the Software & Information Industry Association
http://studentprivacypledge.org/?page_id=45

Continued on page 4

Endnotes

1 Of the 79,790 security incidents reported world-wide in 2016, only 165 occurred in education (65 of which resulted in confirmed disclosure). Verizon, 2015 Data Breach Investigations Report, available at http://www.verizonenterprise.com/DBIR/2015. A risk management consulting company calculated 3,930 data breaches in 2015, less than 14% of which involved education. RiskBased Security, Data Breach QuickView, available for download through https://www.riskbasedsecurity.com.

2 Chloe Albanesius, "Pa School Sued (Again) Over Webcam Spying," PC Magazine (June 8, 2011) www.pcmag.com/article2/0,2817,2386599,00.asp

3 Stephanie Simon, "The big biz of spying on little kids," Politico (5/17/14), available at www.politico.com/story/2014/05/data-mining-your-children-106676

4 Id.

5 Id.

6 Personally identifiable information includes data that can directly identify a student, such as a name, and also data that can be used indirectly to identify an individual student, such as date of birth or mother's maiden name.

7 National Association of State Boards of Education, Policy Update v. 22, No. 4 (June 2015), available online at www.nasbe.org/wp-content/uploads/2015-State-Legislation-6.9.pdf

8 Protecting Student Privacy While Using Online Educational Service: Requirements and Best Practices, PTAC-FAQ-3, February 2014. http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf

9 Protecting Student Privacy While Using Online Educational Services: Model Terms of Service, PTAC-FAQ-4, January 2015, http://ptac.ed.gov/sites/default/files/TOS_Guidance_Jan%202015_0.pdf