K-12
BLUEPRINT
A planning resource for personalizing learning

Federal and State Student-Data Privacy Overview

toolkits

There is an unprecedented push to create, implement, enforce or refine industry-wide standards and legislation to protect student data.

While the use of student data for education has skyrocketed due to increased personalization of learning, the issue of protecting student privacy has, sadly, lagged behind. Yet due to increased awareness, there is an unprecedented push to create, implement, enforce or refine industry-wide standards and legislation to protect student data.

Speaking to the U.S. House Education and Workforce Subcommittee on Early Childhood, Elementary, and Secondary Education and the U.S. Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies in June, 2014[1], Mark MacCarthy, Vice President of Public Policy for the Software & Information Industry Association (SIIA), feels that, while the industry needs to take more personal responsibility for protecting student privacy, more legislation is not only unnecessary, but could prove harmful:

"[The] SIIA agrees that the obligation to safeguard student data privacy and security means that continued review and enhancements are needed in the framework of our policies, practices and technologies...However, we do not think that new federal legislation is needed at this time. The current legal framework and industry practices adequately protect student privacy. Moreover, new legislation creates substantial risks of harm to the innovative use of information that is essential to improving education for all students and ensuring U.S. economic strength in an increasingly competitive global environment."

Making a Federal Case of Privacy

Jim Shelton, acting deputy secretary at the U.S. Department of Education, maintains that, in addition to the creation of ethical standards within the ed-tech industry, an evolving and layered federal, state, and local regulatory framework is needed to protect student data:

"Our new guidance is an attempt to build on the foundation that FERPA [the Family Educational Rights and Privacy Act] and COPPPA [the Children's Online Privacy Protection Act] provide and have provided for years. We are evolving as the landscape changes and our hope is that states, districts and schools are paying attention to us and taking appropriate steps themselves. But there is a huge variance in how districts are protecting themselves and their students, which is in some ways completely understandable given the differences in their size and capacity, so that means we need federal and state regulatory frameworks that help close those gaps while also maintaining a healthy environment for new more effective solutions. This challenge is not unique, but it is pressing because our children's safety is at stake. That said, we also don't want unwarranted panic to result in bad legislation or regulation that robs us of the opportunity for the potentially fantastic advancements ed-tech holds."

www.k12blueprint.com

In February 2014, the U.S. Department of Education (along with other education and industry groups)[2] issued a collection of student-data privacy guidelines called *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* to help define student privacy rights under FERPA and COPPA. The guide recommends that schools and districts be aware of other relevant federal, state, tribal, and local laws and have policies and procedures to evaluate proposed online educational services.

The State of Student Safety

Many lawmakers are working hard on the state-level to bolster student digital privacy protection and specify best practices for shielding that data in a variety of different ways.

More than 170 bills on student data privacy and security were considered by state legislators in in 2015. Guidance issued by the Federal Trade Commission and US Department of Education in that same year represents the prioritization of efforts to help states, districts, and those closest to students keep student data safe and secure.

Student data privacy was also a priority issue in state legislatures in 2016. The privacy conversation has evolved since 2014, and now states have the ability to borrow from each other: California's 2014 Student Online Personal Information Protection Act (SOPIPA), the first to attempt to legislate the permissible activities of school service providers in the digital age, served as a model for many states this session. Most of the states that passed new laws in 2016 had already passed a student data privacy law, a sign that states are building on their efforts.

1 https://thejournal.com/articles/2014/06/25/ed-tech-leaders-testify-in-congressional-hearing-on-student-data-privacy.aspx

2 http://blogs.edweek.org/edweek/DigitalEducation/Student%20Privacy%20and%20Online%20 Educational%20Services%20%28February%202014%29. pdf