

SB 599 (2014): Student Data & Cloud Computing

Summary: SB 599 would require that a cloud computing service provider that contracts with a K12 school district to only use student data in accordance with the terms of its contract, and would prohibit the service provider from using data for a secondary purpose, such as advertising, creating an individual profile, or selling the data.

In practical terms, many school systems use cloud computing to provide access to administration, teachers, and students to a suite of tools to be used in the educational setting -- such as email, document & presentation creation, spreadsheets, etc. Examples of such tools might include Microsoft Office or Google Apps for Education.



What is "cloud computing"? Utilizing technology "in the cloud" generally refers to storing and accessing data and programs over the Internet, instead of on a computer's hard drive. The "cloud" is a metaphor for the Internet.

JCOTS held two meetings devoted to both SB 599 and peripheral issues raised by the bill relating to student data, cloud computing, privacy, and security. JCOTS heard from the following individuals, businesses, and organizations:

- Joel Reidenberg, Professor of Law and Director of the Fordham University Center for Law and Information Policy. The Center has conducted extensive research on issues related to student privacy and cloud computing.
 - Ben Schrom, the Program Manager for Google Apps for Education
 - Paige Kowalski, Director of State Policy & Advocacy for the Data Quality Campaign (DQC). DQC advocates for the effective use of data to improve education and student achievement, while at the same time recognizing the need for schools to be good stewards of student data -- which includes taking steps to promote privacy, security, and transparency in data collection.
 - The Virginia Department of Education
 - Mark Schneiderman, Senior Director of Education Policy for the Software & Information Industry Association
 - Chesterfield Public Schools, Chesapeake Public Schools, Henrico Public Schools, and Fairfax County Public Schools
-

There are several other bodies of law that are relevant to any discussion of student data. These laws include:

- **The Family Education Rights and Privacy Act** (FERPA): Federal law that governs access to student records. The law was originally enacted in 1974, when student records were contained on paper files, but applies to electronic records. The law parents (and students over 18) the right to inspect, review, and correct student records. Schools must have written permission to release records to anyone other than the parent or eligible student. There are a number of exceptions to this general rule. Schools may release "directory information" regarding students, but must inform parents of directory information and provide an opportunity for the parent or eligible student to opt-out of the release of directory information. Recently, the federal Department of Education has hired a Chief Privacy Officer to assist with the application of existing law and the development of best practices as they relate to student privacy, cloud computing, and the use of longitudinal data systems.
 - **The Protection of Pupil Rights Amendment** (PPRA): Federal law that ensures that schools must obtain written parental consent before collecting certain information from students that would reveal political affiliations, income, mental and psychological problems, etc.
 - **The Children's Online Privacy Protection Act** (COPPA): Federal law that governs collection of personal information from children by certain websites. If a website, or a portion of a website, is directed towards children under 13 years of age, or if a website operator has actual knowledge that it is attempting to collect personal information from a child under 13 years of age, the website must obtain parental consent to collect the personal information.
 - **Pupil Records**: Article 5 (§ 22.1-287 et seq.) of Chapter 14 of Title 22.1 of the Code of Virginia. This Article sets forth in Virginia law limitations on the dissemination of student records, and largely mirrors FERPA.
-

Several other states have addressed issues related to student data privacy in the past year. A variety of approaches have been pursued. Most laws adopted in other states do not deal solely with issue of cloud computing contracts, but address broader issues and concerns related to data collection and usage and student privacy -- such as the use of longitudinal education data systems and the data that may be collected and shared; the adoption of privacy & security policies; notification to parents in the event of a database breach; etc. The matrix below summarizes, at a high level, the approaches taken by these other states. A description of each category is included following the matrix.

	Limits commercial use of data	Other contract elements	Breach notification	Index of data elements in state longitudinal system	State data security plan	Local data security plan	PPRA-like provisions	Penalties	Privacy Official
CA	✓	✓	✓						
CO				✓	✓		✓		
FL							✓		
ID	✓	✓	✓	✓	✓	✓		✓	
IN		✓	✓		✓		✓		
KS		✓	✓	✓	✓	✓	✓		
KY	✓	✓	✓		✓	✓			
LA	✓	✓					✓	✓	
MO		✓		✓	✓				
NH				✓					
NY		✓	✓	✓	✓	✓		✓	✓
NC		✓	✓	✓	✓				
SC						✓			
SD					✓		✓		
TN	✓						✓		
WV		✓	✓	✓	✓		✓		✓
WY			✓		✓				

* Not included in matrix: Maine legislature adopted a study resolution in 2014 to study and make recommendations regarding cloud computing, privacy, security, collection of student data, use of social media, etc., in the education setting.

Key to table column headers:

Limits commercial use of data: The language in each state that limits commercial use of student data differs. Some states take an approach similar to that of SB 599, and prohibit commercial use by third parties. Other states simply adopt the general premise that student data may not be used for commercial purposes by anyone -- the state, the local school district, a contractor, etc. California goes beyond just limiting the commercial use of data by contractors with a school. It prohibits the operator of any website, application, etc. targeted to the K12 audience from using data for commercial purposes or from selling personal information related to the users (this approach is a twist on the federal COPPA approach).

Other contract elements: Several states have adopted language that would require that a contract with a third-party provider contain certain express conditions, such as a security plan for the protection of data, procedures for notifying the school district of a data breach, provisions relating to ownership of data, and/or data destruction & disposition requirements.

Breach notification: Several states have adopted provisions requiring parental notification in the event of a database breach or unauthorized access to identifiable student data. Virginia currently has a general database breach notification law, but it would likely NOT apply to a breach involving student data because the notification is linked to breach of information such as social security numbers or financial account information that could lead to fraud or identity theft.

Index of data elements: Most states, including Virginia, have implemented a state-level longitudinal data system from students around the state. The provisions noted in this column of the matrix require publication of the list of data elements collected and maintained in the system. Many of the state laws also require notification and/or approval of the state legislature to add additional data elements. As noted, Virginia has a longitudinal data system, but it is not codified.

State data security plan: Several states require the state department of education to adopt security and/or privacy policies -- this would largely apply to longitudinal data systems. Some of these states have specific requirements that must be included in the plan, such as planning and protecting against database breaches, data disposition and destruction, and security audits.

Local data security plan: Some states require each school division to adopt a data security and/or privacy plan.

PPRA-like provisions: Many states have adopted limitations mirroring the PPRA limiting the mandatory collection of certain information without written parental consent. Some states go further than the PPRA and also limit collection of biometric data.

Penalties: A few states impose civil monetary penalties for failure to comply with the legislation's provisions. Louisiana's statute also would allow for up to three years imprisonment for third-party contractors who do not comply with the security and privacy provisions set forth in the law.

Privacy Official: New York and West Virginia both require the designation of a state-level official who is responsible for overseeing and serving as a resource regarding the privacy and security of educational data.