Schools' Data Dilemma

It's a balancing act when it comes to who should be allowed to use, manage and dispose of the vast amount of student data piling up in cyberspace.

BY SUNNY DEYE

Sunny Deye is a program principal in NCSL's Education Department.

Oklahoma Representative David Brumbaugh (R) was concerned when he learned that students' personal information might be shared with private, out-of-state companies without the parents' or guardians' knowledge or consent.

Representative David Brumbaugh Oklahoma

"I had been hearing more and more from parents about the data schools gather on our children, what is passed on to the state and federal governments, and how that data could be used—and by whom," Brumbaugh says.

What he heard prompted him to introduce legislation in 2013. "It was the critical first step in developing a set of comprehensive and strict privacy controls on student data collected by Oklahoma's public school system," he says.

The Student DATA Act prohibits releasing student information without state approval to ensure that the Education Department releases only aggregated data and nothing that can be linked to a student. Little did he know then that his bill would be the first of what has become a wave of measures addressing how states, districts, schools and online service providers use, manage and dispose of student data.

Twenty-one states followed Oklahoma's lead and passed 26 bills in 2014, reflecting the increasing complexity of protecting the privacy of student data. Last year, 15 states passed 28 bills addressing a range of related policy issues, gathering the best ideas from other states into comprehensive legislation.

"Sharing of data should have a public purpose."

REPRESENTATIVE DAVID BRUMBAUGH, OKLAHOMA

There are many good reasons to collect and use data. Parents can use the information to support their kids' academic growth at home. Teachers use data to design effective instruction and individualized lessons. Policymakers use data to allocate resources fairly and craft important laws.

There are also, however, plenty of reasons to ensure that student data are stored safely.

The digital revolution is changing the nature and quantity of student data. Gone are the days when student files were stored in a locked cabinet in the school office and shredded or recycled on a reg-

> *"Just like we keep kids physically safe in schools, we need to do the same with their information online."*
>
> SENATOR JOHN ALBERS, GEORGIA

ular schedule. Today, student information is stored on school and district computers, in state education department databases and across the Internet with a variety of online service providers. Managers face a dynamic, ever-growing mountain of data stored on multiple platforms, with many users and owners, that is much more difficult to protect.

Digital Data—A Whole Different Thing

The digital revolution is also changing learning environments. Schools, libraries, museums and community centers are upgrading technology so young people can access digital tools throughout the day, creating new opportunities to learn at any time, any place and any pace.

Senator
John Albers
Georgia

Georgia, for example, is moving away from traditional textbooks and striving to be "all digital by 2020," says Georgia Senator John Albers (R). Digital textbooks don't go out of date, he says, and will be less expensive in the long run than printed textbooks, which "you can't search and you can't zoom in and zoom out of. You can't use textbooks to do a virtual science experiment or an interactive video, which can give you immediate remediation."

What Albers likes most about digital textbooks, he says, is that they're the "great equalizer" for all students, no matter whether they're urban or rural, rich or poor. "Technology—with unlimited access for all students—bridges the gap and allows students to do more."

But along with all those digital tools come concerns about privacy and transparency. As a result, many state lawmakers have followed Oklahoma's lead in modifying their own data standards to ensure students know what is being collected about them and what is being done to protect their privacy.

"Just like we keep kids physically safe

What Is Student Data?

Teachers, school administrators, online educational service providers and government agencies collect data on students in many formats, though the type of data, and who can access it, varies. The data include:

- Academic information—growth, courses taken, enrollment locations, grades, graduation status
- Assessments—results from quizzes, tests, and interim and annual evaluations
- Actions and activities—attendance, behavioral citations, extracurricular activities, program participation
- Demographics—age, race, gender, economic status, special education needs
- Teacher observations and interactions
- Homework from students
- Educational applications that track students' work online

Who Owns the Data?

Parents and students. In Utah, families even receive virtual backpacks to keep track of it all. Utah introduced the country to the "student achievement backpack" concept when the Legislature passed a 2013 bill that gives access to a student's secure and confidential electronic records to the parent or guardian. An authorized user may only access data that is relevant to the user's school or district. The backpack concept keeps the digital record with the student through his or her educational development, while giving parents or students some control over who can access the information.

Georgia took a direct approach, giving parents the rights to the records the school or local board of education maintains on their children. They can request electronic copies at any time.

"Parents have a right to review any data they have," says Georgia Senator John Albers (R). "It's part of good transparency."

in schools," says Albers, "we need to do the same with their information online."

Online assessment vendors defend their practices as secure. They usually collect only anonymous demographic information—race, gender, economic status, languages spoken, etc., and nothing that is personally identifiable, like Social Security numbers, home or online addresses, social media accounts, criminal history or any other "nonacademic information," including gun ownership or sexual behavior.

"We want to be very clear and transparent about the types of data we do not collect," an official from the company that conducts Colorado's education assessments told attendees at a public hearing in February, as reported in the Colorado Springs Gazette.

"There's no stealth technology or monitoring, no cameras on devices during testing and no keyboard monitoring."

State Policy Approaches

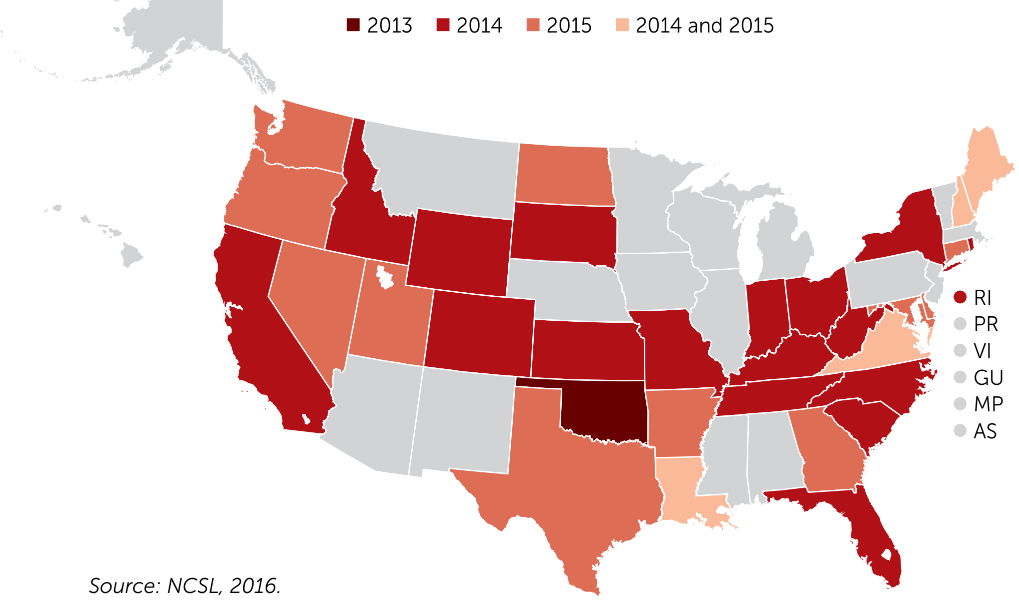
As these issues become increasingly complex, state legislatures are structuring legislation so that the people who need it can obtain complete and relevant information in a timely manner, without violating students' privacy. Policies vary but, generally, require schools to maintain some level of transparency for students and their parents by clearly communicating to families what kind of information they collect, why they collect it, how they use it, with whom they share it and how they protect it. Legislation also usually clarifies that students, parents, schools and policymakers can use students' personal data to support their learning and assist their teachers.

In 2015, states began to put it all together, gathering the best ideas from other states into comprehensive student privacy legislation. The Georgia law, for example, states, "Student information is important for educational purposes, and it is also critically important to ensure that student information is protected, safeguarded, kept private and used only by appropriate educational authorities to serve the best interests of the student."

The law includes strong language about what its intent is, combines the privacy and security obligations of the state education agency, and clarifies the state's expecta-

New Problem, New Solutions

Thirty-three states have passed legislation in the last three years to protect the privacy of students' personal data.



Source: NCSL, 2016.

Policy Questions to Ponder

Before considering legislation, lawmakers may want to discuss the following questions.

- **What is the purpose of privacy policy?** Idaho's bill, for example, expressed a commitment to privacy, while acknowledging the educational value of effectively using data.
- **What data are collected and by whom?** Is it the correct data and is it available to those who can use it to improve student success? Colorado's law requires the State Board of Education to publish an inventory of the types of student information currently in the data system and of any data proposed for inclusion.
- **Who is responsible for developing and overseeing the data's security?** States have selected a variety of gatekeepers—from state leaders to advisory boards—who will be responsible for ensuring privacy and security. West Virginia's Student Data Accessibility, Transparency and Accountability Act, for example, requires the state superintendent of schools to appoint a data governance officer.
- **Do districts have the information, capacity and resources to protect student data?** Virginia now requires the state Department of Education to develop and annually update a plan for protecting student data held by districts.
- **Do privacy requirements apply to private sector companies that provide digital services to students?** California legislators decided their law should apply to operators of K-12 websites, online services and applications, and to mobile applications, whether or not they contract with schools. The legislation stipulates that student data may be used only for school purposes. Providers are prohibited from using, sharing, disclosing or compiling personal student information for commercial purposes, including advertising and profiling.

The Data Quality Campaign and the Consortium for School Networking developed 10 Student Data Principles to guide the use and protection of students' personal information. Read all 10 at ncsl.org/magazine.

tions of companies that have access to student data.

Albers says the bill had two purposes: to address student data privacy and digital classrooms. He says the key points of the law include:

- Officials at the state Department of Education must create an inventory of what data they're collecting and why. Supporters of the law want to avoid collecting certain information (for example, religious preference or political affiliation) just because it's always been done that way.
- Any state agency or city or school system that houses student data must have a good security plan in place—the same type of plan that exists for financial and health care information.
- Service providers are prohibited from using data for any purpose—such as profiling or target advertising—other than educating the student.

Virginia's new law requires the state Department of Education to develop and annually update a model security plan for the protection of student data held by school districts or divisions that includes guidelines on who has access to student data, how frequently privacy and security audits should be conducted and what procedures to follow in the event of a breach, among other concerns.

Maryland's Student Data Privacy Act of 2015 requires operators of Internet sites, services and applications to protect certain student information from unauthorized use, to maintain security procedures and to delete certain student data. Sponsor Delegate Anne Kaiser (D) says the law aims to ensure that safeguards are in place when contracts are signed.

Delegate
Anne Kaiser
Maryland

Nobody can disagree with the premise of protecting student data, she says. "This bill helps ensure that there won't be targeted advertising due to a student's activity online."

The Issue Lives On

Protecting student data isn't a one-time event. Even in states where legislation has been enacted and security measures are now in place, there are ongoing efforts to help districts and schools comply with new laws. In Oklahoma, where lawmakers inspired nationwide activity on student data privacy in 2013, work is underway to add protections.

Oklahoma Representative Jason Nelson (R), who co-sponsored Brumbaugh's 2013 bill, conducted an interim study in 2015 to continue the conversation about keeping student data safe. Brumbaugh supports the effort. "It's one thing to be the first ones out there, but another to be sure we are advancing the core concepts and building upon successes," he says.

"Instead of using the data for policy and policy promotion, we need to spend more time helping local districts disseminate and use data to benefit learning while providing security for students and families."