The State Education Standard
The Journal of the National Association of State Boards of Education

Classroom View of What Data Can Do
Addressing Equity with Data
Balancing Use and Protection of Student Data in Georgia
Oklahoma and California’s Leading Legislation

... and more

THE POWER OF DATA
features

6 What Data Can Do: A Teacher’s View of Digital Tools for Formative Assessment
Digital devices and applications offer the best way for savvy teachers to gauge student learning and adjust instruction. Kerry Gallagher

10 Georgia’s Balancing Act: Using, Protecting, and Legislating Student Data
The state navigates through stormy legislative sessions to arrive at a sound framework for managing its education data. Dana Rickman

14 Using Data to Promote Educational Equity
Good data will be central to whatever course states choose in addressing gaps in achievement and disparities in assignment to special education. Brenda Shum

18 The Federal Role in Student Data Privacy
Two experts, two perspectives. Khaliah Barnes & Paige Kowalski

21 Student Data Privacy: Going Beyond Compliance
Addressing parents’ fears that student data will be abused requires states to shift toward proactive management of education records. Elana Zeide

25 Data Privacy Laws Follow Lead of Oklahoma and California
States pass student data privacy laws that echo provisions first laid down in two states. Amelia Vance

28 Learning from Student Data
There are good ways to address parental concerns about student data. Opting out of data collection is not one of them. Kobie Pruitt

departments

2 editor’s note
3 news & notes
4 we, the media
5 NCOSEA voice
31 the NASBE interview: Aimee Guidera
36 from the director’s desktop
Two images of the power of education data emerge from Kris Amundson’s interview with the head of the Data Quality Campaign, Aimee Guidera. Everyone can agree that data collection is a tool that serves states’ students, educators, and policymakers. But depending on where they sit, some see student data as a hammer and others as a flashlight.

Given that many teachers have criticized the use of some types of student data as an input into accountability systems, a teacher with a “flashlight” point of view kicks off the issue. Kerry Gallagher paints a picture of a classroom in which real-time data ignites personalized learning and allows her and her peers to teach more effectively.

Brenda Shum also shines a light on the power of data—in this case its ability to illuminate inequities in education that line up with subgroup differences. She details how ESSA and a new federal rule call on states to shoulder prime responsibility for addressing inequality in schools, and she argues that you can’t craft interventions if you can’t see the problems.

Risks to the privacy of student data present a different sense of data as hammer. The dangers to students are real, and parents are right to be concerned. But the main theme of this issue is that fears of misused data or breaches of school computers should not inspire hasty rulemaking that makes it impossible to harness the benefits of student data.

Kobie Pruitt and Elana Zeide provide two views on key principles that can help state policymakers arrive at a balance that addresses parents’ fears while empowering educators to combine education technology and student data to help children learn. Pruitt explains why policies that let parents opt out of data collections are a nonstarter, and Zeide urges states to go beyond the compliance that federal law requires and craft proactive, transparent policies that include teacher training and student voices.

Dana Rickman and Amelia Vance write about states that have led the way on student data privacy. In different ways, Georgia, Oklahoma, and California have all attempted to achieve a balance between protecting data and ensuring educators can use those data for students’ benefit. And while the federal government has not caught up with the flurry of state legislature and rulemaking, they have a key role to play. Paige Kowalski and Khaliah Barnes offer two perspectives on what that federal role should be.
News & Notes

Congress has taken up reauthorization of the Perkins Career and Technical Education Act for the first time in nearly 10 years. Senate and House committees were drafting companion bills in April that they may consider this spring. If they do, the full Senate and House may consider CTE legislation before the August recess. Given CTE’s bipartisan and bicameral popularity, there is a small chance the law could pass this year. In a letter to HELP Committee chairs Lamar Alexander and Patty Murray, NASBE called for increased student access to quality CTE programs, better integration of CTE with core academic subjects, more dual and concurrent enrollment programs, expanded business-industry links, and better development for CTE educators.

As part of the fiscal 2017 appropriations process, Congress began this spring to debate funding levels for new programs authorized under the Every Student Succeeds Act (ESSA). In early 2016, House and Senate committees heard testimony from Education Secretary John King and Health and Human Services Secretary Sylvia Mathews Burwell about the administration’s priority education and early learning programs. Final action on 2017 appropriations is not likely until after the election. In the meantime, NASBE has sent a letter outlining suggested spending levels for key programs. NASBE is also working closely with allied groups to ensure Congress provides sufficient funding for Title I, Title II, the Preschool Development Grants program, and the new Title IV program, Student Support and Academic Enrichment Grant.

ESSA gives state boards new chances to assess and align policies to improve student learning and attainment. NASBE recently released a series of policy updates on how to do just that. NASBE’s Standards-Based Leadership Framework comprises six components: student and educator expectations, curriculum design, educational materials, measures of effectiveness, accountability, and professional development. The reports stress that all strategic planning and decision making must link learning standards with related policies in these areas and that there should be coherence across the six areas as well.

A new analysis by NASBE Executive Director Kris Amundson and Gene Wilhoit, executive director for the Center for Innovation in Education, shows that state boards of education have primary authority for choosing their state summative assessment in 32 states. In 45, they adopt the learning standards on which the assessment should be aligned. Noting that states will be making assessment decisions between now and fall 2017, when ESSA takes effect, they offer nine questions state boards should first ask about assessment.

A new NASBE report, Policymaking on Education Data Privacy: Lessons Learned, tracks the evolution of state boards’ authority to issue rules and guidance on student data privacy and offers seven lessons for how to best use this authority (see map). In addition to their increasing legal authority, board members can use their open meetings to push for improved transparency, training, and reviews of draft legislation to ensure that privacy laws thoughtfully protect students but do not obstruct student learning and success.

Student Data Privacy Bills in 2016 (as of April 19).

[Map showing states with pending legislation]
If you learn anything from this issue of The Standard, it's just how integral student data are to education. Researchers need this information to evaluate what's working in education (and what's not). Teachers use it to improve their instructional practice. Parents use it to understand their child's performance in school. And policymakers can't make informed decisions without it. But state policymakers can learn from another valuable type of data: each other's policies and practices.

This month, NASBE is launching its State Policy Database, an online collection of regulations and practices that govern state education systems in all states and US territories. For years, NASBE members have regularly visited NASBE's Health Policy Database to learn about state policies on school nutrition, substance abuse, anaphylaxis protocols, and more. Our new State Policy Database expands to include other issue areas, starting with college, career, and civic readiness. Here, you'll find policies on state academic standards, student assessment requirements, and policies affecting educator effectiveness, such as professional program standards and licensure requirements. We will be incorporating policy areas such as education data privacy and school discipline as well.

What makes NASBE's database unique is its focus on issues that fall under the authority of state boards of education. It is built by state boards for state boards. NASBE's database comprises information drawn completely from public sources. Users can access actual policy with no firewalls to obstruct them. The database allows users to search, scan, and filter policies by state, topic, keyword, and implementing and adopting authority, making it much easier to find information about a specific state, compare a set of states or issues, and verify who holds authority in a given issue area.

That last field of data will be especially useful as states plan for and implement the Every Student Succeeds Act (ESSA). As many of you know, ESSA shifts power back to the states on such things as school improvement, teacher evaluation, and state summative assessments. But few people know who in each state actually gets to make those decisions. In many cases, it is the state board of education.

Did you know, for example, that 31 state boards get to choose their state test? And 45 states boards adopt the state academic standards on which the assessments should be aligned. Both data points are drawn from NASBE's policy database. Access to information like this is important for anyone seeking greater understanding of education policymaking at the state level, and it is doubly important for state policymakers.

Some of the biggest policy decisions require states to balance multiple factors. Having a clear understanding of state laws and regulations governing the education system can help all policy actors—be it the state board, department of education, legislature, or governor—assess their role in the process and find ways to work collaboratively and efficiently to ensure all students receive a world-class education.

To access NASBE's State Policy Database, visit http://statepolicies.nasbe.org/.

We, the Media

Renée Rybak Lang
Communications Director
For all the legitimate, generally accepted, and educationally sound reasons explored in the rest of this issue, schools, districts, and state education agencies routinely collect and store significant amounts of information about students. These collections usually include highly confidential, personal, individual information—and not just on grades and attendance. Data may include individual students’ demographic characteristics, medical issues, behavior concerns, family situations, Social Security numbers, and other sensitive, private information, all of which needs to be safeguarded and protected.

The Family Educational Rights and Privacy Act (FERPA), the comprehensive federal law protecting the privacy of student education records, applies to all schools that receive funds under an applicable program of the US Department of Education. The department publishes guidance on FERPA topics and provides technical assistance to states and districts. But sometimes the competing interests of use and protection collide in the courts, with important results. Morgan Hill Concerned Parents Association v. California Department of Education is illustrative.

In Morgan Hill, parents of 17 children in seven California school districts alleged in a December 2011 lawsuit that the California Department of Education (CDE) failed to comply with its monitoring, investigation, and enforcement obligations under the Individuals with Disabilities Education Act (IDEA) and thus has not ensured a free, appropriate public education to students with disabilities. The US District Court for the Eastern District of California denied CDE’s motion to dismiss or for a more definite statement in March 2013. Discovery matters were addressed during 2014 and 2015, including the entry of a protective order and the development of an e-discovery protocol. The plaintiffs requested access to several CDE databases, including the state’s longitudinal pupil achievement system, testing and assessment databases, and the special education management system.

Because Morgan Hill asserts statewide, systemic IDEA noncompliance and alleges a failure to locate, identify, and refer children with disabilities, the court declined to limit the requested discovery to small groups of districts or students. It instead ordered CDE to produce information regarding children across the entire state. The request implicates over 6 million children who are attending or have attended any California school at any time since January 1, 2008, and more than 1,000 school districts. FERPA permits disclosure of records with personally identifiable information when it is in compliance with a court order. Notice of the request for the databases and the types of information contained therein was provided by publication on websites of CDE and local educational entities.

As a result of objections submitted, the district court amended the e-discovery protocol to permit CDE to maintain custody of one database of the most sensitive information rather than providing a copy to the plaintiffs. Under the protective order, no student’s identifying records will be disclosed to the public, and a limited number of people will have access to the data.

Despite these safeguards, some district personnel and parents have expressed concern about the sheer number of people, databases, students, and districts involved. It will be interesting to watch developments in this case and its impact on the future of educational data collection and use.
My students stroll into my class from the hallway. Some are giggling with friends, some arrive alone with their eyes down, and a one or two always seem to make a grand entrance. No matter how they enter, they all know to sit in their small groups and pull out their phones, tablets, or Chromebooks in our bring-your-own-device (BYOD) classroom. Then they look up at the screen in the front of the room, where a QR code and a shortened URL are posted. A few get up to scan the QR code; the others type the URL into their browsers.

Then they get busy. Today they are playing a game that tests their retention of the content from video clips and primary source readings we analyzed in yesterday’s class. Most are looking at their own screens, but some are peeking at their neighbor’s and are pointing or whispering.

Besides greeting individual students as they entered, I haven’t said anything yet. But I already know exactly what they know. Their answers, right or wrong, are color-coded and appearing in real time on my iPad. I glance at their answers while walking around making small talk with individual kids.

I’m collecting instant formative data. Some of it was collected electronically using the game app I set up for them to play as they entered. Some of it was collected when I observed their body language and facial expressions as they entered the room or in our small talk.

By the time class really gets rolling, I know exactly where my students have misunderstandings and what content they have mastered. I know which students are ready to learn and which have something else on their minds.

What Is Meant by Student Data?

As class starts in schools each day and all over the country, teachers like me are...
relying on data they collect to learn about their students and personalizing learning based on those data. These “daily data” collections are often not considered within the context of policy discussions on student data privacy. When policymakers, parents, and researchers talk about student data, they mostly refer to four general categories:

**health/ability**
medical information, allergies, physical and intellectual disabilities, individual education programs, accommodations

**behavioral**
disciplinary records, behavioral intervention plans, notes on behavior

**academic**
grades, test scores, progress reports

**directory**
name, age, address

These categories are not meant to be exhaustive, but they help identify types of data schools collect. Some data are quite specific and sensitive; some are relatively well known even outside of school. At many student privacy conferences and symposia I’ve attended or in which I’ve participated on panels, however, the instant formative data that classroom teachers rely on daily is not referenced much.

### What Are Formative Data?

Formative assessments are in-class exercises that let teachers and students see where they are and what they need to review. Here are a few key elements:

- Formative data are gathered during the learning process; they are used to track progress while students are learning skills and mastering content.
- Low stakes attach to them; they don’t count toward a grade or only as a very small percentage.
- Immediate feedback is possible; teachers can share the results of the assessment with the student right away.
- Teacher and students modify their approach to the content based on the resulting data.

The low stakes and immediacy of formative assessments are what make them about monitoring, and not testing, student learning. This process of learning, assessing, discussing, planning, and learning again is a continuous, real-time feedback loop. It leads to deeper understanding of content and mastery of skills.

Digital tools are making it easier than ever for teachers to gather and analyze formative data. Paper exit slips can take a classroom teacher upward of an hour to sort and graph after just one day of classes. But now, that same teacher can pose a question out loud to the class and ask students to type answers on their mobile phones and hit send. Instantly, the educator knows which students understand and which do not. They can then apply last-minute lesson plans or homework assignment interventions on the fly.

### Teachers and Students Assess Benefits

Elizabeth Solomon, a high school Latin teacher in Massachusetts, includes quick formative activities in the slides she uses to structure her lessons. “I embed questions within existing presentations so that students remain engaged and participatory throughout a class which was, traditionally, much more passive for them,” she says. The bonus for her is that she can see her students’ answers immediately on her laptop. They are engaged and she can instantly identify what they have not understood.

Even Elizabeth’s students agree that submitting their answers and learning how their classmates are thinking helps them stay on track. A junior says, “It’s a great way to have more interactive learning.” His classmates adds, “It feels more like a game. It’s like the teacher and the students are all working together even though we are all on our own devices.”

Student engagement is a substantial benefit, but Elizabeth also knows she is meeting students’ learning needs faster than ever before. “Because the questions are distributed throughout a presentation, I can recognize immediately when the class understands something and is ready to move on to the next step in the lesson. And if they don’t understand, I don’t overwhelm them with additional information that they are not ready for.”

Another Latin student says he better understands how he and his classmates are doing.
explains: “I can use a picture or a screenshot, I can use a clip from YouTube, and I can add my own material and modify it for the lesson. So I can differentiate for the level of the class.” For example, Glenn’s students learn about algebra by watching and calculating speed and distance from skateboarding videos.

When Glenn mixes open source multimedia content with digital formative math problems, his students get a chance to practice what they are learning and find out how they are doing right away. “My students can open it right up in the classroom; we can project their work on the board for discussion. I can modify the questions on the fly or probe their thinking in real time to correct misconceptions.”

Glenn has realized long-term benefits to tracking student learning data with formative assessment tools. He explains, “This information can be displayed anonymously for class discussion, and it can be stored, tracked, and analyzed over time. I can feed it right back into my unit and lesson planning, adjusting my class in real time to meet my students’ needs.” Glenn is able to share this data with his students and their parents as needed so that all stakeholders are informed.

Removing Anxiety

Derek Larson, a fifth grade teacher in Utah, also knows where his class stands. “They’re just playing a game,” he says. “My students are too busy playing that they forget they are showing me in real time what ideas and concepts they need more help with.”

In his middle school life science class, the seats are empty. Students are up and moving. They are using their iPads to respond to questions about cell organelles set to music and video on the big screen. As their results are displayed, they cheer!

Each time her students’ excitement builds, Nicole reels them in by asking why a certain cell organelle fills a particular need. Hands are up all over the room.

In classrooms across the country, digital tools are making this kind of exciting learning environment possible more often, and teachers need less preparation time. Nicole can give her students feedback more often. “Using technology has increased the number of formative assessments that I can give without requiring me to correct more papers.” The digital tools aggregate, sort, and color code the data. Visually, Nicole knows instantly which parts of the content need more study and which parts her students have already mastered.

Passionate About Math in Middle School

From our first conversation, I wanted Glenn Blakney to be my child’s math teacher. He is passionate about making his middle school students experience math rather than merely learn about it.

His latest approach uses open educational resources with digital formative assessment. He explains: “I can use a picture or a screenshot, I can use a clip from YouTube, and I can add my own material and modify it for the lesson. So I can differentiate for the level of the class.” For example, Glenn’s students learn about algebra by watching and calculating speed and distance from skateboarding videos.

When Glenn mixes open source multimedia content with digital formative math problems, his students get a chance to practice what they are learning and find out how they are doing right away. “My students can open it right up in the classroom; we can project their work on the board for discussion. I can modify the questions on the fly or probe their thinking in real time to correct misconceptions.”

Glenn has realized long-term benefits to tracking student learning data with formative assessment tools. He explains, “This information can be displayed anonymously for class discussion, and it can be stored, tracked, and analyzed over time. I can feed it right back into my unit and lesson planning, adjusting my class in real time to meet my students’ needs.” Glenn is able to share this data with his students and their parents as needed so that all stakeholders are informed.

These simple and fun formative assessments help my young students stay more engaged and active while I’m able to get the information I need.
level, Derek’s students do not have BYOD or one-to-one devices, so he uses paper cards that his students hold up to show what they have learned. He uses his own tablet to scan their cards and collect data. He is able to export their answers to a spreadsheet and use it more for detailed planning as well as on-the-spot interventions. “My students respond better to these amazing types of formative assessment because it’s less risk and less worry,” he says.

Implications for State Boards of Education

It is essential to remember these lightbulb moments when discussing the risks and rewards of classroom data. Without the digital formative assessment tools and data that Elizabeth, Nicole, Glenn, Derek, and I have, we would not be able to personalize learning for our students. It would be impossible to track their progress so quickly or easily. Since formative data are usually not used for grading, they are shared only between teacher, student, and parents. The teachers who rely on these data can give their students immediate feedback and support, and they would not be able to do their jobs as well without it.

Educators are invested in what is best for their students both inside and outside of their classrooms. But while teachers do engage in professional development on how to collect and interpret formative data to benefit student learning, they typically do not get similar opportunities to learn how that data can be used by others who have access to it. By providing district and school leaders with the time and resources to inform teachers about the power of educational data both in and outside the classroom, state policymakers can help teachers protect students better.

When education agencies and advocates think of student data, they often think of the information that is reported to state agencies: census information, student health records, and academic achievement. Policies that secure those data cannot be so restrictive that classroom teachers are prohibited from tracking daily data from formative assessments and communicating that information to their students. For instance, when the vetting process for a digital tool is too cumbersome or lengthy, teachers cannot get access to the tools they need in time and lose the opportunity to collect, analyze, and adjust instruction quickly based on formative data. Classroom data help teachers know their students better, help students track their own progress, and the resulting communications help provide parents with a better understanding of what their children are doing in school every day.


Policies that secure those data cannot be so restrictive that classroom teachers are prohibited from tracking daily data and communicating that information to their students.

Kerry Gallagher is a digital learning specialist at St. John’s Prep in Danvers, Massachusetts, and director of K-12 education for ConnectSafely. Kerry taught middle and high school history in bring-your-own-device public schools for 13 years, and her classes were paperless. Find Kerry at @KerryHawk02 and www.KerryHawk02.com.
By combining an overall vision for the use of data, a commitment to protecting student privacy and data integrity, and supportive legislation, Georgia emerged as a leader in the effective use of student data. But it easily could have gone another way. None of the three elements could be taken for granted when Georgia set out to develop its state longitudinal data systems over a decade ago.

A key challenge in Georgia was the entanglement of questions concerning what data should be collected and why with a contentious debate over the Common Core State Standards. The multiyear dispute surrounding Common Core, which included discussions of the proper role of the federal government in education policy, nearly derailed the statewide longitudinal data systems (SLDS).

SLDS ensure that states manage, use, and analyze education data effectively to support instruction and policymaking. Educators need information to help every student succeed, and at the same time, states need to protect student privacy and institute security measures to protect the integrity of the data.

While Georgia had been working on a longitudinal data system since the mid-2000s, it was only completed under the federal Race to the Top grant (RT3). In its grant application, the state had already set a clear vision for what it wanted to accomplish. Georgia listed five goals:
1. Set high standards and rigorous assessments for all students—leading to college and career readiness.
2. Prepare students for college readiness, transition, and success.
3. Provide great teachers and leaders.
4. Provide effective support for all schools, including the lowest-achieving schools.
5. Lead the way in science, technology, engineering, and mathematics fields.

To achieve all five, Georgia required a robust state data and information system that would transcend all state education agencies. State leaders from the Governor’s Office, the Governor’s Office of Student Achievement, the Georgia Department of Education, and other education stakeholders including the Georgia State Board of Education (SBE) submitted a winning application during the second phase of the competition in June 2010. That year, Georgia was awarded $400 million over four years to implement its detailed plan for public school improvement.

Included in the RT3 grant was implementation of Common Core English language arts and mathematics standards, as well as the overall vision for data usage:

- make educational data available that supports cross-agency analysis;
- establish an environment that will support data storage and access over time;
- establish an environment that will be valued by the community it supports and require minimum resources to maintain.

As part of the grant, Georgia proposed development of an accessible statewide longitudinal data system that would inform and engage stakeholders, support decision makers, and enhance overall instructional effectiveness.

There were 33 projects under the grant, but Common Core implementation was among the most prominent. From that point forward, the Georgia public and some Georgia lawmakers linked Georgia’s data systems project to the Common Core and federal dollars. Subsequent debates over the appropriate collection and use of data would continually return to those two points.

Two Data Systems

Georgia developed and implemented two related state data systems. Georgia’s Academic and Workforce Analysis and Research Data System (GA•AWARDS) provides researchers and policymakers information about programs and overall effectiveness. Its SLDS, called Path to Personalized Learning, provides students and educators with seamless access to data that can inform instruction.

GA•AWARDS is the anchor for Georgia’s data collection and usability to track overall student achievement and inform policy. It links data across 10 education-related agencies, beginning with early learning data and spanning data collected by the Georgia Department of Labor (DOL).

The system provides data matched to the needs of each agency and allows agencies to examine trends. Georgia’s agencies use GA•AWARDS to construct and make publicly available state, district, and school report cards and to answer a range of potential research questions: Which educator preparation programs are most effective? What was the education background of students who experienced the least difficulty in transitioning to college? How does Georgia’s pre-K program affect later student achievement? Are Georgia’s public college graduates working in Georgia?

Knowing the answers to these and other critical outcome questions allows SBE members and other key stakeholders to continuously improve policy, instruction, operations, management, resource allocation, and overall effectiveness of the system.

Georgia’s Path to Personalized Learning contains individual student data for pre-K through twelfth grade. This system enables educators to provide individualized instruction and receive targeted professional development. It delivers student data, curriculum standards, and instructional resources directly to teachers and parents through their district’s student information system.

Taken together, GA•AWARDS and the Path to Personalized Learning provide powerful tools to inform student instruction and increase public awareness of how Georgia’s schools are performing.
The bill imposed limits on data collection, usage, and technology that would have rendered the data system useless and made online learning challenging.

### Two Student Data Privacy Bills

Throughout 2013 and 2014, Common Core dominated education policy discussions in Georgia. During the 2014 legislative session, Senate Bill 167 sponsored by Senator William Ligon came close to passing but was ultimately defeated in the House. Not only would SB 167 have severed Georgia from the standards, it would have banned student assessments that reflected any national or multistate standards and imposed limits on data collection, usage, and technology that would have rendered the data system useless and made online learning challenging. In addition, it would have created a redundant review and advisory board to influence the state board's curriculum decisions.

The primary objection to which the bill gave voice was the perceived loss of local and state control over decisions related to curriculum and testing. While SB 167 was defeated, what did pass during the same session was establishment of a House study committee to review the origination of the Common Core standards, investigate their federal ties, and review any contractual agreements between state education agencies and the federal government. This review took place throughout 2014.

At the same time, Governor Nathan Deal charged the SBE to conduct its own review of the Common Core standards. In response, the board conducted 14 public comment meetings (one in each congressional district) and implemented a detailed survey of teachers and other educators.

By December 2015, the House committee had concluded that decisions on standards should be left to the SBE, and the SBE's evaluation gave legislators confidence in the board's decisions concerning standards. In testimony during House hearings, presenters were able to clarify confusion concerning the Common Core and perceived data requirements related to the standards, and they also explained the purpose of the two data systems.

During the 2015 legislative session, two competing data bills were introduced. Senator Ligon introduced SB 157, a slightly modified version of the data portion of SB 167 from the previous year. At the same time, others in Georgia wanted to focus on the security, appropriateness, and ethical use of the data managed in Georgia's two data systems. Therefore, a bill ultimately called SB 89, first introduced in the House by Representative Buzz Brockway, focused on these issues. The Georgia Partnership for Excellence in Education joined with a coalition that included the Georgia Chamber of Commerce and the Foundation for Excellence in Education to advocate for passage of SB 89 not only to protect the powerful data systems the state had worked hard to put in place but also to ensure security and student privacy.

The two bills took different approaches. SB 157 used an approach that the national advocacy group Data Quality Campaign termed prohibitive, meaning that it sought to limit or outright ban collection of certain types of data (biometric data, in the case of this bill) or data for specific uses, such as predictive analytics. This bill both limited the types of data that could be collected and restricted interagency use of data, which was a priority in Georgia. These limitations would have severely hampered education policy research conducted using GA•AWARDS data and impeded online delivery of instruction.

SB 89 was dubbed by the Data Quality Campaign as a governance bill, which delineated procedures, supports, and roles and responsibilities of agencies and personnel to ensure data would be used appropriately. Three interrelated concepts marked the legislation: intent, governance, and transparency.

The bill's authors clearly laid out its intent in the opening sentence: "to address issues relating to the advancement and use of technology in schools." The opening paragraph highlighted the importance of data in improving student learning while acknowledging the need for accessibility, security, and transparency. Transparency was paramount. The competing bill's supporters voiced explicit concerns about the use and purposes of collected education data. There was the feeling that Big Brother was monitoring students and their families.

SB 89 governed state and local activities as well as online service providers. To develop, implement, and oversee state and local activities, the legislation established a chief privacy officer, a senior position within the Georgia Department of Education. This officer's primary duties include the following:

- establish departmentwide policies to ensure privacy protections relating to the use,
collection, and disclosure of student data;

- assess the impact of legislative proposals, regulations, and department program initiatives on privacy protections;
- establish and operate a Privacy Incident Response Program to ensure that incidents involving department data are properly reported, investigated, and mitigated;
- establish a model process and policy for any parent to file complaints of privacy violations;
- provide training, guidance, technical assistance, and outreach to build a culture of privacy protection, data security, and data practice transparency to students, parents, and the public.

The legislation also called for state and local districts to develop detailed security plans. These include guidelines for authorizing access, security audits, responses to protocol breaches, retention and disposal policies, and security training. The governance protocols for the state and districts also differentiated between the types of data that can be collected from those that are unnecessary and do not belong in an educational record, such as families’ political affiliation, voting record, or religion.

The bill extended to private third parties as well and required technology providers that work with schools and districts to develop appropriate security procedures. It also prohibited them from selling personal information about students and using the data for targeted advertising. While both bills reflected concerns about private companies’ use of education data, the legislation that prevailed found a compromise that allowed access sufficient to enable companies to provide educational services without exposing students to direct marketing campaigns or increased risk for data breaches.

SB 89 also focused on transparency. It tapped the chief privacy officer to ensure that policies and procedures governing the state data system would be publicly available. It also mandated a data inventory and a corresponding index of data elements to clarify for the public what data are and are not being collected. Finally, the legislation explicitly established a parent’s right to review their child’s education record, required schools to provide electronic copies of student records to parents upon request, and set up an appeals process to correct inaccuracies within the record.

With the debate around Common Core largely settled by the start of the 2015 legislative session, the conversations around these two bills could focus on their individual merits. Citizens and policymakers needed reassurances that education data were being used appropriately and securely. Many also wanted assurance that Georgia was making its own decisions with regard to data and not being directed by the federal government.

With passage of this bill, Georgia was able to stave off the more limiting bill that could have undermined education data’s ability to inform instruction and policy. The new Student Data Privacy, Accessibility, and Transparency Act, signed by Governor Nathan Deal in May 2015, helps to ensure the privacy and confidentiality of students’ personally identifiable information, mitigates risks related to the intentional and unintentional use of data, and establishes clarity of roles and responsibilities around data use.

Georgia has tackled the complicated student data question by balancing usability, privacy, and security. Although this issue requires constant attention, the state’s experiences can serve as a model for other states facing similar challenges.

3The report card contains test results as well as other school-performance information relevant to student achievement and graduation. It also includes school-, district-, and state-level reports concerning accountability, Georgia and national achievement tests, indicators of success, student and school demographics, personnel and fiscal indicators, and comparison data. Data are updated annually and made available on the Office of Student Achievement website: https://gosa.georgia.gov/contents-report-card.
6Ibid.

The legislation that prevailed found a compromise that allowed access sufficient to enable companies to provide educational services without exposing students to direct marketing campaigns or increased risk for data breaches.
Data plays a starring role in promoting educational equity, and data-driven decision making begins with good state policies. With the recent passage of the Every Student Succeeds Act (ESSA) and a proposed federal rule to address racial disproportionality in special education, states will shoulder increased responsibility for eliminating educational inequities.

**Accountability under ESSA**

With ESSA, Congress signaled a fundamental shift in the federal government’s role in public education. Moving forward, states will have more flexibility than they experienced in the No Child Left Behind (NCLB) era on issues related to accountability, resource allocation, and teacher evaluation. States will be responsible for establishing their own accountability systems, though these must be submitted to and approved by the US Department of Education.

State accountability indicators must include proficiency in reading and math; high school graduation rates; English language proficiency; valid, reliable, and statewide student growth indicators for elementary and middle school students; and at least one other indicator of school quality, which might include safety or school climate, student engagement, or postsecondary readiness (see box on types of data states collect). Although ESSA reduces the exclusive reliance on tests as a measure of success, academic indicators must still be weighted more heavily than nonacademic indicators.

However, ESSA did not abandon NCLB’s commitment to using accurate, transparent data to measure equity. Annual statewide assessments are still required in order to provide objective, comparable data on how students are performing. Indeed, schools are now required to disaggregate data for homeless students, military-connected students, and foster children in addition to subgroups NCLB already identified.

ESSA contemplates reliance on academic and nonacademic indicators of performance, and it requires comprehensive public reporting on outcomes and opportunities to learn, including per-pupil expenditures and access to curriculum. District and state leaders must act if any subgroup is consistently underperforming by identifying interventions for the lowest performing 5 percent of its schools and those with the highest achievement gaps. But states and not the federal government will determine what those interventions will be.

Data that reveal state trends and patterns offer the means through which school boards and districts can take advantage of new opportunities ESSA offers to ensure that all students are meeting learning standards. States can use this information in several transformative ways:

- They can use the new accountability systems they devise under ESSA to incentivize best practices, not just penalize school failure.
- They can use data to inform strategies targeted to the needs of specific subgroups. ESSA expects subgroups that are further behind to make more rapid progress in order to close proficiency and graduation gaps.1
- In order to do so, states can adopt a set of principles to inform the accountability system they propose under ESSA. These should incorporate feedback from parents as well as educators and administrators: Greater data transparency will build trust within the community.
- They can make sure that data collection aligns with the state curriculum so that instruction matches student learning objectives. Test results and other data must be reported and analyzed in a timely manner and accessible format.

---

**Using Data to Promote Equity**

Good data will be central to whatever course states choose in addressing gaps in achievement and disparities in assignment to special education.

_by Brenda Shum_
Disproportionality in Special Education

In 2013, the Government Accountability Office reported that inconsistent state definitions of disproportionality and limited oversight were hindering states from identifying racial and ethnic groups that were overrepresented in special education classes. Students of color with disabilities are more likely to be suspended and expelled than white students with disabilities. Exclusionary school discipline is associated with lower academic performance, higher dropout rates, lower graduation rates, and future disciplinary exclusion and involvement with the juvenile justice system.

Accordingly, the US Department of Education issued a proposed rule in late February to ensure equity under the Individuals with Disabilities Education Act (IDEA). States must determine whether significant disproportionality on the basis of race or ethnicity is occurring within the state or its school districts. The proposed rule, which is open for public comment, requires states to adopt a standard methodology to identify significant racial or ethnic disproportionality in the identification, placement, and discipline of students with disabilities.

Under the rule, states would use a risk ratio and select a threshold to determine significant disparities. Disproportionality in special education exists when a subgroup of students is over- or underrepresented in a specific category or area. This ratio must be determined with stakeholder input. Moreover, significant disproportionality will be analyzed by the incidence, duration, and type of disciplinary practices for students with disabilities, including suspensions and expulsions. When significant disproportionality is identified, states must review and revise district policies. States must also communicate that districts can use IDEA funds to create comprehensive, coordinated early intervening services for students receiving special education as well as for students who have not yet been deemed eligible.

What does this mean for states? In order to comply, states would need to collect and analyze the relevant data. But while the risk ratio analysis will show states how much more or less likely a student in a specific subgroup is to be identified for special education or subjected to discipline, it will not necessarily reveal why. States will need to work with districts to decide how best to intervene based on this analysis.

Role for State Boards

States boards and their members are uniquely situated to facilitate long-term, sustained improvements in student achievement by setting clear expectations for how local schools and districts will be evaluated and what data will be relevant to that process. State boards can engage multiple stakeholders in identifying the metrics for student achievement.

States can also support schools and districts as they seek to report their data in a more meaningful way. For example, dashboard systems and early warning indicators allow all stakeholders to understand and use performance data to identify appropriate and timely interventions, encouraging transparency and accountability.

Data analysis can be overwhelming and intimidating. Schools and districts may resist what they perceive to be the increasing burdens associated with rigorous, comprehensive data

Three Types of Data

States typically seek three types of data that influence student achievement: inputs, educational processes, and outputs. Educational inputs may include variables such as student background and socioeconomic status, or teacher experience or level of training. Educational processes involve curriculum, instruction, materials available to a student, or the level of teacher and parent involvement in decisions. Outcomes measure the results of both the input and process variables and typically rely on student tests, observations, or survey results. Different data may be gathered in different ways and offer specific insights into which students are achieving and why. Accordingly, a state will likely use multiple means of assessing student performance and school quality.
More on Discipline Disparities and Data

Based on data collected through 2012 on up to 49 million students, the US Department of Education’s Civil Rights Data Collection (CRDC) exposed the extent to which zero-tolerance discipline policies were disproportionately affecting minority students. Across all age groups, black students were suspended and expelled at a rate three times greater than white students.

CRDC data also showed a striking disparity in preschool suspension: While black children make up 18 percent of preschoolers, they account for more than 40 percent of out-of-school suspensions. The pattern continues throughout primary and secondary education, with 16 percent of black students being suspended compared with 5 percent of white students. This information prompted the US secretary of education and attorney general to issue formal recommendations for changing discipline practices, which districts have been implementing.


Making Data Matter

Data can be used to sustain best practices in curriculum and instruction, identify factors that contribute to inequities, identify effective strategies, allocate resources effectively, and design modifications in the education environment. Data-driven decision making may be framed by smart state policies, but the efforts to adopt policies and build data systems will be for naught unless there is also a commitment to actually use available data to improve schools.

ESSA and the proposed federal rule implementing IDEA raise the profile of education data. These changes present new opportunities to improve how schools serve the most vulnerable and disadvantaged students. State leaders must be prepared to devise and implement accountability systems, academic standards, and assessments, which data will fuel. With accurate data, states and districts can focus time and resources on interventions with the highest likely impact on student success.

State boards can adopt robust measures of student performance and school quality that go beyond test scores, including student and parent surveys, college readiness benchmarks, teacher satisfaction, and community engagement. Making sure there are clear, accurate, and accessible data represents the first step in addressing the complex issues related to student performance and in creating more equitable school systems.

Making Data Matter

Data can be used to sustain best practices in curriculum and instruction, identify factors that contribute to inequities, identify effective strategies, allocate resources effectively, and design modifications in the education environment. Data-driven decision making may be framed by smart state policies, but the efforts to adopt policies and build data systems will be for naught unless there is also a commitment to actually use available data to improve schools.

ESSA and the proposed federal rule implementing IDEA raise the profile of education data. These changes present new opportunities to improve how schools serve the most vulnerable and disadvantaged students. State leaders must be prepared to devise and implement accountability systems, academic standards, and assessments, which data will fuel. With accurate data, states and districts can focus time and resources on interventions with the highest likely impact on student success.

State boards can adopt robust measures of student performance and school quality that go beyond test scores, including student and parent surveys, college readiness benchmarks, teacher satisfaction, and community engagement. Making sure there are clear, accurate, and accessible data represents the first step in addressing the complex issues related to student performance and in creating more equitable school systems.

The efforts to adopt policies and build data systems will be for naught unless there is also a commitment to actually use available data to improve schools.

Brenda Shum is director of the Educational Opportunities Project at the Lawyers’ Committee for Civil Rights under Law. She can be reached at bshum@lawyerscommittee.org
Today’s classrooms are equipped with Fitbits, tablets, mobile tracking apps, digital posters, and other technology to support classroom instruction. And some classes are conducted virtually so that all information is transferred digitally. Indeed, big data in the classroom has raised big problems for student privacy. Schools collect, digitize, and store sensitive student data on cloud-based services, creating a perfect storm in which student records are disclosed widely for many purposes without meaningful accountability.

Unsurprisingly, schools, companies, and others that have amassed student information have been unable to adequately safeguard it. They simply cannot keep up with all the data they have collected and have routinely experienced data breaches. These breaches have compromised grades, student financial information, Social Security numbers, and even special education records.1

Congress charged the US Department of Education (ED) with enforcing the Family Educational Rights and Privacy Act (FERPA)—the main federal student privacy law—when it passed the law in 1974. Yet ED rarely investigates alleged FERPA violations or finds that schools have violated the law.2 Nor has the Federal Trade Commission, which has authority over the actions of private companies collecting student information, stepped in to investigate the behaviors of these companies. More can and should be done at both the state and federal levels to protect student privacy.

More can and should be done at both the state and federal levels to protect student privacy.
Nearly all education stakeholders can agree on two things. First, using data to personalize learning for all students is the wave of the future and not a fad. Second, safeguarding student data privacy is both critical and urgent.

Happily, the two are not mutually exclusive. Districts, states, and the federal government have a role to play in both ensuring the privacy and security of students’ personal information on the one hand and, on the other, in building trust that student data are used appropriately. In fact, privacy safeguards and effective data use are mutually supportive. Strong safeguards enable schools to confidently make the case to parents that student data are being used safely in beneficial ways.

Trust Matters

Education data can benefit everyone. Educators have richer, more useful information than ever before to tailor their practices to students’ individual needs. Parents can make better informed decisions about their children’s learning. Students can better manage their progress toward their college and career goals. But they will not use data they don’t trust or in an environment that doesn’t value that trust. The immense potential of student data is thwarted when parents, teachers, and school leaders do not have confidence that student information is reliable, safe, and secure.

States and districts can build trust in student data by providing value to parents and teachers (e.g., How does sharing this information benefit my student?) and by being utterly transparent about their policies and procedures (e.g., What data are collected and why? Who has access? How are data shared? What privacy safeguards are in place?). While laws are essential, you can’t legislate trust. It must be built.

A Patchwork of Privacy Laws

Equally as important as building trust is building a strong legal foundation for protecting student privacy. All levels of government—local, state, and federal—are responsible. Rising to the challenge, states have begun legislating around student data privacy. In 2015 alone, legislatures in 47 states introduced 188 bills. States have demonstrated impressive leadership. However, the results are a mixed bag.

State efforts have increased transparency about what data are collected and for what purposes, stronger privacy security laws and policies, clearer governance of data, and more open communication across the field—especially with parents and teachers. At the same time, several states have introduced or passed legislation that would (often unintentionally) limit the use of student data to improve learning and create an undue burden for teachers and administrators, often without actually enacting any significant data protections.

This patchwork of state laws creates an opportunity for the federal government to think critically about its role in safeguarding student privacy. The federal government can be a critical partner in complementing, supporting, and reinforcing state efforts to protect student information. Existing federal laws—including the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and the Children’s Online Privacy Protection Act (COPPA)—offer an important but incomplete legal foundation (as detailed in Elana Zeide’s article on page 21). The federal government should consider how their own patchwork of privacy laws can be amended and implemented better. Ultimately, states and the federal government ought to work together to develop a more streamlined system of legal protection.
A Role for the Feds

Information practices and technological capabilities are light-years ahead of what they were when current federal privacy laws were enacted. Federal action should continue to align and clarify student protections while working to advance the field’s capacity to protect student information. My organization, Data Quality Campaign, has identified three roles we believe the federal government should play in safeguarding student data privacy.

Legislating for the Future. The integration of technology into education has significant implications for the privacy and security of student information, and federal laws haven’t caught up. Student data are now collected, stored, and shared digitally, often in cloud-based systems. While COPPA addresses online privacy, it is not always clear to school districts and educators how the law applies to use of online service providers and applications. And while FERPA has been applied to electronic records in some situations, the law is not designed to cover data collected outside of a student’s official school record. Neither law sufficiently addresses current and potential security concerns related to evolving digital learning environments.

Federal law must be strong enough to protect student information in an increasingly digital school environment yet broad enough to allow states and districts to innovate. Changes to FERPA should recognize the digital environments in which student data are generated and stored, account for schools’ uses of third-party online applications that collect student information, and address the need for security safeguards designed for modern digital environments.

Cross-Agency Coordination and Clarity. States and districts must navigate the protections offered by federal laws: FERPA and PPRA, which are administered by the US Department of Education (ED), and COPPA, which is administered by the Federal Trade Commission (FTC). By coordinating across agencies to provide clarity to those on the ground as to how these different privacy laws work together, the federal government can make this navigation easier. When the federal government provides consistent definitions and standards, states and districts can better understand and build upon this foundation to protect student information.

In particular, ED and the FTC can issue joint guidance to help states and districts implement federal privacy laws and better inform state laws and policies. They can help clarify for the public which federal laws govern student data privacy, their application in school settings, and federal governance of websites and online applications.

Support States and Districts. Individuals in districts and schools need training and support to build a culture of trust and implement best practices in data privacy and security, and the federal government already has begun to develop some tools to support local infrastructure and capacity building. The Privacy Technical Assistance Center (PTAC), for example, offers a hotline and guidance on issues such as data breach response and model terms of service. But more is needed.

Continued federal attention to the role of states and districts in safeguarding student data is vital. The federal government can support them by providing more tools and resources to help them adopt policies and best practices in transparency, governance, and privacy and security. These supports can also include funding for building capacity—especially through related training and professional development—throughout the system, from the state to the local, school, and classroom levels. The newly minted Every Student Succeeds Act (ESSA) takes a step in the right direction by explicitly listing data literacy and data privacy trainings as allowable uses of professional development grant (Title II) funds for states and districts.

Moving Forward

Federal leadership in student data privacy can reduce the burden on states by aligning and clarifying the current patchwork of federal laws and by helping advance the education sector’s capacity to protect student information. Given the upcoming implementation of ESSA and a recent focus on this issue by members of Congress and the White House, there is a unique opportunity for federal action. A solid legal foundation at the federal level clears the path for states and districts to take on the hard work of fostering trust around education data use. When parents, teachers, and school leaders trust that the information is reliable, secure, and protected—and is being used in an environment that values their trust—then the immense potential of education data to improve student learning can be unleashed.
With Edward Snowden’s 2013 revelations about surveillance by the National Security Agency, privacy once again became a hot topic in public debate, but this time in a world increasingly mediated by digital tools. The debate quickly extended beyond broad consumer and citizen concerns to focus on student data privacy. Since 2013, most states have considered one or more bills to protect student data, with many giving state boards of education more authority in this arena. The best of this legislation goes beyond compliance to better address stakeholders’ fears.

States that take this approach have adopted two key practices in implementation of new state laws: They develop a comprehensive understanding of what information state and local education agencies (SEAs and LEAs) hold, and they communicate clearly with parents about what happens to student data, how these data are protected, and how data collections benefit students.

**Technology Moves ahead of Policy**

Anchored by the Family Educational Rights and Privacy Act (FERPA), the existing student data regulatory system satisfied stakeholders for almost 40 years in part because of the inherent limitations in how paper-based student records could be shared, used, and repurposed.

Federal law has not kept pace with the technological advances that have transformed education data collection, 

**Addressing parents’ fears that student data will be abused requires states to shift toward proactive management of education records.**

by Elana Zeide
to be used and privacy-focused questions about how such information should be handled in education environments. As a result, many arguments for “student privacy” in fact revolve around opposition to data-reliant education policies such as adoption of the Common Core and not specific information-handling practices in schools and classrooms.

Separating privacy from broader education policy is essential for state boards that wish to have constructive conversations with diverse stakeholders. It is important to remember—and to remind others—of this distinction. Privacy involves practices governing the sharing, use, protection, and retention of personal information. Because digital platforms have become integral to all aspects of society, it is fair to say that schools, districts, and state educational agencies will still have access to a significant amount of student information even in the absence of data-driven education policies. Educators and administrators will still need to ensure that appropriate rules and policies are put in place to protect student data regardless of its broader role in the education system.

Other Concerns

Safety and Security. Another set of issues involves preventing unauthorized data access, which the ease of information flows through and outside school networks make possible. Parents worry that school data collection will provide information to would-be predators, and they fear that data breaches will lead to identity theft.

Commercial Exploitation. Much of the student privacy debate concerns the individuals and entities with which schools share personally identifiable student information. As discussed above, FERPA limits school disclosure to some extent but doesn’t address the ways that entities can now repurpose information collected in the course of providing schools educational services. Parents wonder if these secondary uses will be used to conduct experiments or generate profit and what the effect might be on students.

Unintentional Effects of Educational Use. Parents fear that information monitored by schools in the name of security and bullying prevention will be used against students. Stakeholders worry that data collected by educational actors will become digital dossiers, the modern-day equivalents of the proverbial...
permanent record, and foreclose students’ future opportunities because of early mistakes or missteps. They fear the repercussions of information sharing even within institutions. They wonder if historical performance data will become self-fulfilling prophecy.

FERPA’s Flaws

Traditional student privacy regulatory frameworks like FERPA do not adequately address all of these concerns. FERPA’s fundamental structure was built in an era of paper records and is a poor match for today’s concerns. Consequently, it is difficult to interpret and apply the statute to today’s technology. FERPA also fails to address important issues that arise from technological advances. So while the federal law should expand technical definitions and the scope of protection around personally identifiable information, such updates would only touch the surface of current concerns.

More important, in its focus on disclosure, FERPA doesn’t address educational actors’ own information practices. Because it delegates the bulk of data-related decision making to educational institutions without strong, accompanying transparency requirements and accountability mechanisms, FERPA cannot ease stakeholders’ fears.

FERPA’s transparency obligations are minimal, requiring only that educational actors provide student and parents with access to personally identifiable student information. Under the school official exception in annual FERPA notices, schools and districts must also include information about their nonconsensual disclosure policies, but these notices tend to be so broad as to provide little concrete information about the data schools collect and share and the purposes this collection and sharing serves.

The same is true of information use on the agency level. The Department of Education revised FERPA’s regulations in 2008 and 2011 to better accommodate the reality of digitized records and networked information flow by creating explicit rules allowing SEAs to share personally identifiable student data more easily with researchers and vendors managing state longitudinal data systems. These regulations use contractual provisions, instead of requiring “direct control,” to ensure recipients protect and use covered information appropriately. Many advocates and parents are not aware of what concrete limitations these contracts impose.

Schools, LEAs, and SEAs must also provide parents with the opportunity to challenge student data. Given the quantity, granularity, and dispersal of collected student information, however, it is difficult to do so in a meaningful manner.

Another important FERPA feature is its compliance orientation. While experts often speak of FERPA as permitting this or prohibiting that, it is technically a statute that conditions federal funding on compliance with its provisions. The consequence for noncompliance is withdrawal of federal funding. However, given the drastic nature of that measure and the way that might ultimately harm the very students the statute seeks to protect, the US Department of Education administers FERPA with an eye toward encouraging compliance rather than punishing noncompliance.

Education institutions and agencies must demonstrate a policy or practice of consistent violations before they will be sanctioned. In effect, education actors get benefit of the doubt. The statute presumes that they will comply to the best of their ability and that this effort will be enough to prevent harm. Stakeholders may not operate with the same faith.

In the absence of rigorous institutional transparency, stakeholders have almost no sense of, as well as no say in, the information practices related to student data. Without a clear understanding of schools’ privacy practices and no evidence of consequences for information misuse or mismanagement, stakeholders may get a sense that schools are not being diligent about how they protect and use student data. This understandably creates a sense of unease.

Stakeholders are neither Luddites nor helicopter parents. Given the fast pace of technological development and new analytical tools that reveal increasing amounts of information and can be applied to more and more uses beyond their original application, it is impossible to predict what data collected today will reveal tomorrow and how those data will be used. It is logical to hesitate in the face of such uncertainty, especially in the absence of a sense of transparency or accountability accompanying these tools and technology.
Beyond Compliance

FERPA governs education agencies’ disclosures to outsiders but does not restrict their own practices regarding data collection, use, protection, and retention. This fact, coupled with its limited minimal transparency obligations and reticence about enforcement contribute to stakeholder resistance. It is only natural to fear that which is unknown and over which one has no control. Accordingly, I advise individuals and entities with access to personal student information to go beyond mere compliance toward proactive management of information and privacy. Adopting and articulating public policies can go a long way in reassuring parents that education agencies are thoughtful stewards of student information.

Because education technology offers such promise, proponents often lose sight of the fears it prompts. When proponents speak of the benefits of putting data-driven technologies in place, the message may not resonate with parents, who are concerned with the effects on individual students in the present rather than those in the future or the education system as a whole. State longitudinal data systems, for example, have not been promoted as ways to improve the immediate educational quality or opportunities of students today. Viewed from that perspective, parents’ hesitation makes eminent sense: Why put a child at potential risk for rewards that she won’t reap?

A Three-Tier System

I find it helps for policymakers to view proposed information practices and privacy policies through a three-tier framework when crafting contracts, more information privacy rules, and communicating with educators and stakeholders. First, examine practices from the perspective of a student data subject or his parent. Second, consider the ramifications of new technologies and policies on students collectively. Third, examine how information use promotes extra-educational goals such as research and profit making. Understanding these separate strands may not assuage all stakeholders, but it will prepare education agencies to respond to pushback against new technology and information practices.

Best Practices

Inventory and Transparency. In the absence of control over their child’s data, parents need information about what is happening to feel secure. Stakeholders may interpret the lack of readily available information or transparency not as reticence or omission but as deliberate deception.

Transparency first requires a thorough inventory of the data a school or education agency collects, the paths through which it flows, and the rules that govern it. Ideally, education agencies would then publish what information they collect and why, how it is used, who can access it, and how it is protected.

Very few schools, districts, or states have this level of transparency. And they likely would find the idea daunting: No one wants to trigger a backlash. However, openness will ultimately foster trust. Detailed transparency may be challenging at first, but such an investment in establishing community and stakeholder trust is worth it.

Privacy Policies and Principles. Given the amount of detail involved and the pace at which it changes, it is best to begin by articulating broad approaches to data—principles such as data minimization or restrictions on commercial repurposing. For example, schools should create explicit rules regarding employee data-sharing authority and accountability, including policies covering adoption of data-sharing technologies in classrooms that frequently do not require administrative approval. By setting out practices and privacy policies beforehand, schools and education agencies will likely receive the benefit of the doubt.

Another helpful tactic is to communicate the need for information practices to be standardized. It may be difficult for those outside the school system to understand the confusion that would be caused if parent preferences dictated data flow for every decision.

Designate a privacy point person or position. Many states have created chief privacy officer positions to be this point person. Even if decision-making authority is more broadly dispersed, there should be a specific place where stakeholders can turn for privacy guidance and clarification. Teachers...continued on pg 35
Since 2013, one or both of the student data privacy laws passed in Oklahoma and California have shaped bills that were introduced in 35 state legislatures and became law in 14 states. The Oklahoma law, passed in 2013, focuses on actions of staff at the school, district, and state levels. The California law, passed in 2014, regulates nongovernmental actors, such as education technology companies, which gain access to student data in the course of their work with schools.

**Oklahoma’s Focus on Transparency**

Oklahoma’s Student Data Accessibility, Transparency, and Accountability Act (known as the Student DATA Act) arose just as privacy concerns about student data were beginning to surface. According to Linnette Attaí, founder of education technology compliance consultancy PlayWell LLC, “When this climate of data privacy first emerged in its current form, this was one of the key questions: How are states understanding what data they have?”

The law assigned extensive responsibility to the Oklahoma State Board of Education, requiring it to set policies and establish safeguards for state-collected student data. Before its passage, student data was handled “largely at the staff level within the department, outside of any public process or public scrutiny,” according to Oklahoma State Representative Jason Nelson, coauthor of the bill. One of the concerns that parents and privacy advocates most frequently voiced was the lack of transparency about how government was using and protecting student data. By giving this authority to the state board, Oklahoma enhanced the transparency of its student data privacy decisions and created a model for the country.

The Student DATA Act set in stone best practices that were echoed in bills introduced across the country. It required the state board to develop policies and procedures that complied with all relevant privacy laws; ensure that data are accessible only to the people who need it to do their jobs, like a child’s teacher; ensure vendor contracts include provisions that safeguard privacy and included penalties for noncompliance; and submit an annual student data privacy report to the governor and legislature. The law also restricted the state’s ability to collect unnecessary and especially sensitive data from districts, such as Social Security numbers and biometric information.

Oklahoma’s transparency requirements are especially praiseworthy; they emphasize the need for public disclosure of policies. “States have been using education data obviously for quite a while to improve the education services that they provide and support their students, but they haven’t always done a good job of communicating how they were using information and how they were governing it and protecting it,” said Rachel Anderson, senior associate of policy and advocacy at the Data Quality Campaign. “This model was really innovative in that it really gave the public a sense of what was going on and ways that they could help hold the state accountable for their data activities.”

Transparency is not only a best practice, it can be the only way to push back against inaccurate information about student privacy that parents may gather from other sources. Chip Slaven, counsel to the president and senior advocacy adviser for the Alliance for Excellent Education, said schools want to avoid parents hearing information only from “the talk radio show or from some Internet blog that’s not informed.” He added that schools should ensure parents “know where to go when they have questions and have some sense of comfort that there are efforts being made to protect their child’s information.”

---

**Data Privacy Laws Follow Lead of Oklahoma and California**

Across the country, states have engaged in the sincerest form of flattery in passing student data privacy laws that echo provisions first laid down in two states.

by Amelia Vance
maintain adequate security and delete student information when requested by the school or district. In order to balance privacy and beneficial uses of technology, the law explicitly allowed third parties—as authorized by the school—to use student data for adaptive or personalized learning. For example, a math games company could create a profile of a student that tracks what the student had accomplished previously and adjust the game so the math questions are at the right level for that student.

If third parties violate the law, SOPIPA allows the California attorney general to bring a case against the company in court. “SOPIPA paved new ground,” said Zeide, who added, “The devil will be in the details of implementation.” For example, vendors can disclose sensitive information for research, provided there are privacy and security protections in place, but it is unclear what the law considers a legitimate research purpose. Such research might be undertaken to improve a product, but it also could further understanding of “how education is working and how students are actually learning,” said Brendan Desetti, director of education policy for the Software and Information Industry Association. Most experts said there will be no regulations to clarify such aspects of SOPIPA, so it is very likely some definitions will be clarified by judges as vendors are brought to court for alleged violations.

Since 2014, 26 states have introduced SOPIPA-style bills, with seven of those bills becoming law (see map).

California Restricts Private Firms’ Access

Regulating government actions was important but not sufficient for privacy advocates, who were also uneasy about the increasing amount of student data held by private companies. A 2014 survey from Common Sense Media revealed that 90 percent of parents surveyed were concerned about “how private companies with noneducational interests are able to access and use students’ personal information.” Many of those parents indicated they wanted to make it illegal for companies to sell students’ private information to advertisers and ensure tighter security standards for student data held “in the cloud.”

In response, California passed the Student Online Personal Information Protection Act (SOPIPA) in 2014. It was the first law to specifically regulate third parties, like education technology companies. “Privacy protections that apply directly to noneducational actors [such as SOPIPA] are a more effective way to address stakeholder fears about commercial actors than trying to do so indirectly by restricting how schools share student data,” said Elana Zeide, a privacy expert from the NYU Information Law Institute.

Even though federal law already prohibited companies from advertising to students, SOPIPA went further, requiring that third parties not sell student data or use student data to create a “profile” on students for a noneducational purpose. The law also required that vendors maintain adequate security and delete student information when requested by the school or district. In order to balance privacy and beneficial uses of technology, the law explicitly allowed third parties—as authorized by the school—to use student data for adaptive or personalized learning. For example, a math games company could create a profile of a student that tracks what the student had accomplished previously and adjust the game so the math questions are at the right level for that student.

If third parties violate the law, SOPIPA allows the California attorney general to bring a case against the company in court. “SOPIPA paved new ground,” said Zeide, who added, “The devil will be in the details of implementation.” For example, vendors can disclose sensitive information for research, provided there are privacy and security protections in place, but it is unclear what the law considers a legitimate research purpose.

Such research might be undertaken to improve a product, but it also could further understanding of “how education is working and how students are actually learning,” said Brendan Desetti, director of education policy for the Software and Information Industry Association. Most experts said there will be no regulations to clarify such aspects of SOPIPA, so it is very likely some definitions will be clarified by judges as vendors are brought to court for alleged violations.

Since 2014, 26 states have introduced SOPIPA-style bills, with seven of those bills becoming law (see map).

What’s Next?

Forty-nine states have introduced student privacy bills since 2013, with 35 states passing at least one law. However, some of these laws may not fully protect privacy, and others’ strictures are accidentally inhibiting districts from, in one case, enrolling students in a state scholarship fund.

Recently, the American Civil Liberties Union (ACLU) dipped its toes into the student privacy debate, introducing a model bill in nine states that could add privacy protections for students in schools that provide each of them a computer or tablet. However, some of the ACLU language may trigger accidental consequences. For example, a requirement that parents opt in every time the
example, SOPIPA does not clearly define what is meant by targeted advertising, Attai said. “It’s a new term,” she said. “We’ve always referred to advertising as behaviorally targeted or contextually relevant, and those come with definitions that have been in place at the Federal Trade Commission level through reports, cases, and other legislation. It’s been very challenging for industry to understand what needs to be in place in order to be compliant with SOPIPA.”

Kobie Pruitt, education policy manager at the Future of Privacy Forum, said that he would encourage state policymakers to look closely at definitions that could be too broad. As an example, he cited a Florida law that banned biometrics, which caused problems for special education classes that routinely used video cameras and recordings to help students. “If the student has a speech impairment, for example, ‘a voice recording could be used to help chart their progress and show the successes teachers are having with that student,’ Pruitt said.

Neither the Student DATA Act nor SOPIPA incorporated language around training teachers and administrators. “It’s very important that we have training as a part of the requirements,” Amelia Vance is NASBE’s director of education data and technology.

...continued on pg 33
The debate about the safety of student data arose quickly, and there are good ways to address parent concerns. Opting out of data collection is not one of them.

by Kobie Pruitt

Learning from Student Data

Just as adults’ personal lives and data increasingly inhabiting online spaces, so are students. While this shift brings many benefits and the possibility of learning tailored to individual students’ needs, it is also brings new challenges. Students create an electronic trail of information that creates an obvious concern: How can they enjoy the better learning outcomes technology makes possible but still maintain control of their data and be protected?

Nearly two years ago, a debate ignited over student information from multiple states and regions being collectively stored with the data repository InBloom. Critics charged that the not-for-profit service provider could potentially sell, misuse, or otherwise put at risk student data it held for schools. Surprised by the backlash, InBloom was ill prepared to explain its services to parents. Critics didn’t trust a third party whose name they didn’t recognize and who didn’t provide any service they could see, or track to a direct benefit for their child’s educational experience.

InBloom looked to school leaders, who were relying on the vendor to support school data handling, analysis, and reporting, to tell parents that nothing had changed. Other ed tech vendors already were managing student data, often storing it with cloud providers rather than keeping it on local servers. Apps and other programs collected student data as they provided educational services. InBloom would join the ranks of outside companies helping schools manage data better.

But school leaders did not have ready answers for the critics. For a small but determined group, InBloom became a target for larger concerns about education reforms generally, in particular questions about curriculum reform or standardized testing. The fact that InBloom’s charitable backers included foundations associated with some of those reforms only served to conflate student data privacy with other hot-button issues.

The resulting pressure found school leaders without clear answers specific to student data privacy concerns. The primary federal law, the Family Educational Rights and Privacy Act (FERPA), enacted decades earlier, was frequently dismissed as out of date. In actuality, however, the US Department of Education has regularly updated regulations under the law multiple times to take into account new technologies and issues. Even so, FERPA regulated schools, not vendors, so concerns were raised that it did not effectively bar companies from misusing education data.

In 2014, legislators in 36 states responded to these concerns by introducing 110 bills related to student data privacy. By the end of 2014, 21 states had passed 24 new student data privacy laws. The following year saw a dramatic increase, with 47 states introducing 188 bills addressing student data privacy. Five months after InBloom closed its doors, California passed the Student Online Personal Information Protection Act (SOPIPA), which put vendor restrictions in place.

Twenty-six
other states subsequently used SOPIPA’s framework in their own student privacy legislation (for more on SOPIPA, see Amelia Vance’s article elsewhere in this issue).

During the same period, education service providers began to take a more public stand to show their support of responsible practices for handling student data. In order to help them build public trust, the Future of Privacy Forum and the Software and Information Industry Association began coordinating with these companies to sign a Student Privacy Pledge. Pledge signers committed to not sell student data, to use data only for purposes that schools authorize, and to refrain from behavioral advertising, among other restrictions. The pledge is a legally binding commitment for the vendors that sign it, enforceable by the Federal Trade Commission and states’ attorneys general. To date, over 230 companies have signed on and the White House has endorsed the pledge and urged every vendor handling student data to make the commitment.

But at the end of the day, there is only so much that vendors, state laws, pledges, or the US Department of Education can do to explain to parents how and why student data are collected and what protections are in place. Those who are trusted with students and their data need to be able to articulate the reasons for data collection and how it benefits students and teaching. When these reasons are not clear, parents question the process and are suspicious of the risks they see, and may begin to question the right of the school or district to collect and hold data about their children.

Between consumers or parties to agreements in other contexts, the exchange of data for a service is a voluntary transaction, and in many cases there are levels of control for what data are provided. In some cases, there is the offer to “opt in” with more information for additional services, or “opt out” for collection or use of data that the user may feel is beyond the scope they are willing to provide. Because of this mindset, some concerned parents have sought these same controls in the student data context — the change to opt in to various school programs or services, or opt out of others. For the most part, however, these are not viable strategies within the primary role of the educational system, and it is important that parents understand the distinction, as well as the limited context in which such controls can be applied.

The collection of student data within the educational system is not a discretionary exchange. In addition to the direct individual record created on each student based on their academic performance within their current classroom or grade level, there is data use to understand how well students perform over time, how well a school system is serving different populations, and how well different educational strategies are succeeding.

At the individual level, processes in a public educational system must be safe and sufficient for all students. If a particular program or activity results in a situation that carries unacceptable risk such that opting out is required, then it is not a program that should be used in the first place. Just as a student cannot “opt out” of being...
marked for attendance or for being graded, the process that collects and records grades and attendance must be sufficient for the protection of all the students’ grades.

Beyond the individual level, there is likewise no justification for allowing individual families the opportunity to withhold their particular records from the aggregated uses of student data. The metrics for how classes, schools, or districts perform must be reliable and accurate. If primarily low-income or, perhaps, high-income students were to opt out, schools and policymakers would be misled as to the real results of the educational system, lacking information that accurately reflects all sectors of the school community.

There are, however, some secondary uses of data where parents can and should make choices, namely, in contexts where any sharing of student data is for purposes unrelated to primary educational activities. Yearbooks, extracurricular activities, or other programs outside the direct educational process are all situations where parents should have the option of how far to participate. In fact, these are the areas where federal law mandates that schools give parents the chance to opt out.

Concerns of frustrated parents over policies they oppose need to be heard and resolved. They should certainly be provided assurances that their children are safe. But their concerns need to be addressed by fixing problems for all students, as part of an educational system that is appropriate for everyone. If a chosen online service or application is too risky, then school leaders must choose a different service provider or refrain from using it.

Policymakers seeking to address parent concern by crafting privacy rules for student data need to consider the full scope of data collection and use to sustain the value of education, and particularly look to avoid the unintended consequences of restrictions written too broadly. Fear should not be the basis of policy development or be allowed to hold back genuine improvements to the educational system.

School leaders, working in partnership with ed tech vendors, owe parents a clear understanding of how and why data are collected and used. A national survey conducted by the Future of Privacy Forum showed that parents support technology in the classroom and the collection and analysis of student data when they understand the benefits for their child and her class or school.4

School leaders must be ready to answer questions by taking advantage of the many resources available. Additionally, if staff at state and local education agencies, and even policymakers and legislators, familiarize themselves with these resources, they will all be better able to help parents understand how schools and states are using data to benefit students and provide better learning outcomes.

Resources

Department of Education PTAC
http://ptac.ed.gov/
FERPA|Sherpa
http://ferpasherpa.org/
Student Privacy Pledge
http://studentprivacypledge.org
CoSN Trust Framework
http://www.cosn.org/Framework
iKeepSafe, FERPA Assessment
http://ikeepsafe.org/privacy/ferpa/
iKeepSafe, California Student Privacy Badge
http://ikeepsafe.org/privacy/california/
Data Quality Campaign, “Roadmap to Safeguarding Student Data,”
http://dataqualitycampaign.org/find-resources/roadmap-to-safeguarding-student-data/
Common Sense Media
https://www.commonsensemedia.org/privacy-and-internet-safety


Pundits have written that the Every Student Succeeds Act may be the most data-reliant piece of legislation ever passed about American education. I would love to hear your reaction to that statement and what you see as the role of data as we move forward with ESSA implementation.

I’m very optimistic that we are entering a new era in which it’s possible to empower all of the stakeholders in education with the information they need and deserve to help support student learning and success.

ESSA represents a pivot from thinking about data as [part of] a compliance exercise, purely for accountability purposes, and starting to think about data as a tool to empower better decision making and to inform continuous improvement. That’s a very big culture change in education. We have always had data, but it’s always been seen as something people have to do, as a hammer. ESSA helps us turn the corner toward creating a culture where we can start using data to personalize learning and as a flashlight to truly inform the decision making of everybody. ESSA does help launch an era of thinking about accountability to fellow citizens, to our neighbors, and, most important, to children.

What are the big questions that state boards of education ought to ask as they move from thinking of gathering data for compliance toward data as a flashlight?

I would say we have to start with asking people what they need and prioritize getting them the information. What I need as a mom is different from what a state board member needs, which is different from what a teacher needs or a school superintendent needs. We need to ask people what questions they have and then we need to map backward and figure out what information those individuals need in their roles. Then we make sure we are collecting the right data, minimizing the amount of data that we are collecting [and] only collecting data that are necessary to answer the priority questions, and making sure we are not just collecting that data but that we are turning it into information. And we are getting that information into the hands of those individual users in a way that’s timely, that’s useful, that’s tailored to those questions they have, and in a way that respects privacy, security, and confidentiality requirements. [We need to] be able to show the value of data and to build trust that this information will be used well and protected.
Thanks to the incredible leadership of state policymakers and district leaders across this country, we have the data. It's sitting there. So now, how do we make sure that we're building the capacity to access [this information and] to use it responsibly and well? We change how we use time and how we use training to make sure that people are well prepared and aren't feeling overwhelmed by the use of data but instead are feeling empowered by it.

*Talk about balancing that tension between protecting privacy and marshaling data and some examples of states that might have tipped too far one way or the other.*

We're never going to be done with privacy, nor should we. It's not something [to] get through and move onto other stuff. As long as we talk about empowering people with quality information, we have to talk about how we protect that information. It's just part of the effective use of data. I won't use data if I don't find value in it and if I don't have trust that it's not going to be used to hurt me. So those two pieces—making sure that people understand what’s in it for them or their children and making sure that they trust it's going to be safe, secure, and confidential—are critical to people's willingness to have data collected and used in education. It's not an either/or; it has to be both.

First, we have the ability to use this information and protect it, but second, we can't afford not to use it to help every child in this country be prepared for success in life. We can't afford to lose a single child in this country, and the power of data is about making sure that at every point in a child's life we know when a child is falling off track.

And when a child is struggling, we're able to figure out what works and what interventions are helpful to get that child back on track. We're able to personalize and tailor learning for every child to excel and meet high expectations.

Yes, we've seen states that have gone draconian and just shut [data collection] down, but I'm heartened that, in most cases, leaders in our states have very much realized that's harmful to children and that's not going to help their states. Leading states like Georgia are, first of all, making a statement about the value of data and understanding that the state will not meet goals of having every child succeed if they don't tap into the power of data and new technologies. Second, states have put in place strong data governance, making it clear who is in charge of making sure that data are kept safe. Where does the buck stop in decisions of who has access to data, how long can it be held, will data need to be destroyed, what are the rules guiding this, and what are the processes in place to update policies and practices? We've seen the rise of chief privacy officers, which is just great.

Third, we absolutely have to recognize that these best practices are going to continue to evolve. Last, [there is] a real focus on training, on those closest to our students and having the most access to data. Anyone who has access to student data has to understand how important it is to keep this data safe and then receive the tools to do that. Georgia has also taken the next step of talking about how to regulate outside partners that are helping to leverage the power of data through technology and also just to keep the buses running.

We've seen hundreds of pieces of [data privacy] legislation introduced over the last three years. At the end of the day, the vast majority of the laws that have been passed have been productive and have changed the tenor of the conversation about data in education. There is only one law on the books from two sessions ago that really has constrained the role of data in Louisiana and put a damper on innovation and the power of data to help kids.

*How would you prepare teachers to make the most of the data that they have available to them?*

You can have the most high-quality data at everyone's fingertips, yet when teachers don’t find value in that information, don’t know how to use it, and don’t trust it, that data won’t change anything. We are working at Data Quality Campaign to make sure teachers see data as a good thing, and that change in perception is what matters. DQC has worked with national organizations, including the teacher unions, to develop a shared definition of data literacy and policy recommendations to make sure every teacher in this country is data literate. Specifically, preparation programs for educators have to prioritize data literacy.
That needs to be one of the core courses as you prepare teachers. It’s important to note that it’s not just assessment literacy; it is much more than a test score. States have to change their licensure and certification policies to recognize and demand data literacy: making sure their teacher force knows how to use information and how to keep that information safe.

If you leave a laptop open on your desk, the data are not secure.

We’ve all attached a wrong attachment to an email or kept someone on an email that shouldn’t have been. They are not malicious mistakes but [reinforce the point that] everyone has a role. For so long, our approach to privacy has been compliance. You would hear people say, “Well, we’re compliant with FERPA.” That breeds trust on no one’s part. Yes, federal laws matter. But we’re truly protecting data when everyone understands their roles and responsibilities. You can’t legislate trust, and trust is about people changing their behaviors.

What is the most exciting thing you see on the horizon?

DQC is launching a policy roadmap for states. We’ll be talking about four policy priorities states should take if they want to leverage the power of data to serve student learning. At this point, only 13 states can guarantee that parents and teachers have access to the information they need on their students. With ESSA, [there is] the opportunity for states to think differently, creating accountability systems and using data to manage for those results. As part of that, we’ll have a more engaged citizenry, especially parents, than we’ve ever had before. When you start giving people the information they need to answer the questions that are foremost in their minds, it changes the conversation, it changes the decisions made, it changes actions and behaviors, and ultimately it changes the results.

Pruitt said. “Because with all these new laws, if teachers don’t know how to navigate the new landscape, I don’t think the laws are going to be that effective.”

Slaven agreed. “Whenever I see a proposal that’s around professional development to help teachers or to help any school official who has to deal with data and privacy … that’s a game changer, he said. He added that most teachers and administrators likely “don’t know a quarter of what they need to know on this issue. So they end up either not worrying about it like they should, or they overcompensate and do too much.”

States that desire a comprehensive and smart approach to privacy, like Georgia and Delaware, have taken the next logical step: passing both a SOPIPA and an Oklahoma-style law in order to maximally protect student privacy while allowing for education technology in the classroom.

This may not be the right approach for all states. Some states, like New Jersey, already had Oklahoma-style regulations for student data in place prior to 2013. But for others, this approach could provide a starting place for states seeking the best ways to balance privacy and innovation.

Experts urge policymakers to first look at what laws or regulations they already have and then to identify gaps: “The answer to solving a problem or issue that is already covered by existing legislation is often not more legislation,” Attai said, “but enforcement of the legislation we do have.”


continued from pg 27...Data Privacy Laws Follow Lead of Oklahoma and California


they even need to collect students’ personally identifiable information. Schools should work to implement privacy enhancing techniques, which minimize or eliminate the need to collect personally identifiable information. Such practices would permit schools to introduce innovative technology into the classroom without having to compromise student privacy. And privacy enhancing techniques, like anonymization, would permit states to achieve their goals of providing effective, equitable opportunities without putting student information at risk.

In 2014, EPIC created the Student Privacy Bill of Rights, an enforceable student privacy and data security framework. The Student Privacy Bill of Rights aims to put students back in control of their data by establishing six practices:

1. **Access and amendment.** Students have the right to access and amend their erroneous, misleading, or otherwise inappropriate records, regardless of who collects or maintains the information.

2. **Focused collection.** Students have the right to reasonably limit student data that companies and schools collect and retain.

3. **Respect for context.** Students have the right to expect that companies and schools will collect, use, and disclose student information solely in ways that are compatible with the context in which students provide data.

4. **Security.** Students have the right to secure and responsible data practices.

The Student Privacy Bill of Rights: A Path Forward

Student data collection raises important questions for state boards of education and schools:

- For what purposes will the school, or school contractor, use the information?
- How long will the student data be retained?
- What security measures are in place to safeguard the information?
- To whom will the information be disclosed?
- And
- Who will be accountable if student data are disclosed or used in impermissible ways?

But even before asking these questions, state boards and schools must first assess if the court never ruled on the merits of whether the department’s FERPA regulations are lawful.

A sea change in student data collection, use, disclosure, and breaches followed in the wake of the FERPA rule changes. Schools quickly adopted the latest and purported greatest in education technology for a variety of purposes, including email services, remote proctoring, and even student social media monitoring. School data collection is now vast and varied, from answers to in-class assignments, to student location information, to contents of emails, to behavioral assessments. Moreover, because schools have relatively few administrative hurdles to disclosing student data, they routinely do so without meaningful oversight, transparency, or accountability.

**Student Privacy Under Attack**

On a daily basis, students are required to turn over increasingly sensitive information. Here are just a few examples of the personal data—driven technology for instruction:

- Oral Roberts University requires all incoming students to wear Fitbit fitness trackers for a grade.
- Proctortrack, a popular remote proctoring service, scans students’ faces, picture IDs, and knuckles to verify student identification for remote test takers.
- GoGuardian permits teachers to monitor students’ classroom laptop screens in real time.
5. **Transparency.** Students have the right to clear and accessible information privacy and security practices.

6. **Accountability.** Students should have the right to hold schools and private companies handling student data accountable for adhering to the Student Privacy Bill of Rights.

As state boards grapple with the complexities of education technology, they should ask the important questions, execute privacy enhancing techniques, and implement the Student Privacy Bill of Rights. State boards and state education agencies can execute privacy enhancing techniques by collecting only aggregated student data. In addition, they should limit student data retention periods.

Moreover, state boards can evaluate whether their policies align with the Student Privacy Bill of Rights. They should ensure, for example, that students and parents have access to any information that states collect. State boards and state education agencies can make sure they are only using data for the original purposes for which they were collected. So if the state collects student data to implement a federal or state law, state boards must ensure that student data are not used for a secondary purpose. State boards and other policymakers should keep in mind the maxim “If you can’t protect it, don’t collect it!”

States must be transparent regarding the types of information they collect, the purposes for which the information will be used, and to whom the information will be disclosed. Above all, state boards must implement accountability mechanisms when collecting student data. A state education chief privacy officer can field student and parent questions and provide oversight for state student privacy practices.


---

Elana Zeide is an attorney, consultant, and Fellow at New York University’s Information Law Institute.

and administrators can turn to this person to evaluate new data-driven platforms, vendors, and policies. Parents can use this contact point to get clarity on privacy practices and protections, provide feedback on existing policies, and register concerns.

**Train and enlist teachers and educators.** As supported by a recent survey conducted by the Future of Privacy Forum, parents often trust individuals more than the “system.” Take advantage of this fact and encourage teachers to share the ways that data-driven technology helps students and makes their jobs easier.

**Educate and engage students.** Students are all too often left out of this discussion. Most are intensely curious to know about their progress and performance, especially relative to other classmates. While this information should be disseminated wisely to avoid social stigma and self-fulfilling prophecies, a little self-knowledge can go a long way in both motivating students and informing them about the data that are shaping not only their education but much of their lives.

While much of this advice may seem like common sense, it is difficult to integrate these ideas into daily institutional practices, given other pressing needs and the tension surrounding student privacy conversations. Consideration, communication, and proactive policies will not magically erase these differences, but they are a prerequisite for more constructive conversations that further the objective on which everyone does agree: an education system that does its best to support student success.
I remember the first time I got the keys to the car, shortly after my 16th birthday. I had taken driver education and had driven with my parents in the car, but this was different. I was behind the wheel and in charge.

It was not, as I recall, a glamorous errand. My mom needed something from the store. Or perhaps my sister needed to be picked up from a piano lesson. I drove slowly and carefully, making sure I didn’t leave a dent. (That would come shortly afterward.)

You probably recall your first time behind the wheel as well. It’s one of those rites of passage that mark our evolution to adulthood.

Education policy is also growing up. After 14 years of an approach to educational accountability that was top-down and federally driven (pun intended), the Every Student Succeeds Act (ESSA) has changed drivers. ESSA transforms accountability from a compliance-driven model (have we checked all the boxes?) to one in which states have the latitude and authority to make key decisions in four big areas:

Accountability. When President Johnson signed the first Elementary and Secondary Education Act, he said it was designed for quality and equality. Those purposes should be the foundation of any state accountability system. While the law does require continued annual testing, states can add other metrics that they believe more accurately reflect state goals. So consider metrics for social and emotional learning or for access to more rigorous coursework.

Assessment. State boards have major responsibilities in state assessments. In 31 states, the board has the authority to select the state summative test, and in six more states, that responsibility is shared with the state education agency (SEA). Boards can make other key decisions: Do they want to give a single test at the end of the year, or do they want to administer smaller assessments throughout the year? Do they want to allow districts to use a nationally recognized test like the ACT or SAT instead of the state test in high schools? Do they want to be part of a pilot to develop alternative assessments such as competency-based or performance-based assessments?

Teacher and Leader Development. Elimination of the “highly qualified teacher” requirement opens up opportunities for states to define what constitutes good teaching. Particularly in areas like CTE or the arts, this should make it easier to bring practitioners into the classroom to share their expertise with students. States will also want to take advantage of the opportunity to devote some Title II funding to teacher and leader development and professional learning.

School Improvement/Turnarounds. ESSA offers real flexibility here. Working with districts, states need only craft an “evidence-based” plan to improve student achievement in persistently low-performing schools or in schools where achievement gaps for one subgroup persist. Naturally, with increased flexibility will come increased responsibility to monitor schools and districts as they develop and implement their plans.

Don’t wait for a self-driving version of educational accountability. ESSA handed you the keys. So get behind the wheel.
FOR TWO OPPORTUNITIES TO INCREASE THE IMPACT OF YOUR WORK ON STATE BOARDS OF EDUCATION

save the dates!

new member institute
july 21–23, 2016
ritz-carlton, pentagon city
arlington, va

annual conference
sheraton kansas city hotel
at crown center
kansas city, mo
october 19–22, 2016
Be NASBE. Be engaged.

Contact Kristen Amundson, NASBE’s executive director at kristen.amundson@nasbe.org, with membership questions.

www.nasbe.org

My state board of education is a NASBE member. So what do I get?

- **NATIONAL MEETINGS** held every year: Annual Conference, Legislative Conference, New State Board Member Institute
- **REGIONAL MEETINGS**, such as ones held recently in St. Louis on standards-based leadership and in Pittsburgh on science standards
- **CONVENINGS** of states that receive competitive NASBE grants
- **NASBE STAFF VISITS** tailored to the needs of specific state boards: on standards-based leadership, school climate, student data privacy, deeper learning, leadership development, board governance issues, strategic planning, and more
- **CONNECTIONS WITH EXPERTS** through publications such as the State Education Standard, webinars, e-newsletters, conference calls, and face-to-face meetings
- **NATIONAL VOICE** on federal education matters before the administration, Congress, and the US Department of Education
- **OPPORTUNITIES TO SERVE** on association committees and NASBE’s board

“We don’t know what we don’t know. In joining NASBE, I discovered what it meant ‘individually’ to be a responsible, accountable member of a state board of education and how ‘collectively’ we can be a more effective, efficient board in our state. I had the opportunity to network with knowledgeable individuals from all over the country on common issues and challenges and have built lasting friendships.”

—Gayle Manchin, past president, West Virginia Board of Education
HOW CAN STATE BOARDS OF EDUCATION STAY FOCUSED ON THE BIG PICTURE?

NASBE’s Standards-Based Leadership Framework is designed to keep states focused on the foundational issues that put student learning standards at the center of their decision making. A new series of Policy Updates highlights six types of policies that must 1) align to learning standards and 2) cohere with each other. Visit www.nasbe.org to learn more.

New Windows of Opportunity Thanks to ESSA

- Leading a Standards-Based System: Aligning Policy to Standards
- Student Expectations
- Teacher Preparation
- Leadership Preparation
- Curriculum
- Materials
- Measures
- Accountability
- Professional Development

reports on the following topics can help boards with the long-term planning that leads to effective education systems

Decision making
Strategic planning