EDUCATION LEADERS REPORT

Volume 2, No. 1

April 2016

Policymaking on Education Data Privacy: Lessons Learned

BY AMELIA VANCE

NASBE | National Association of State Boards of Education

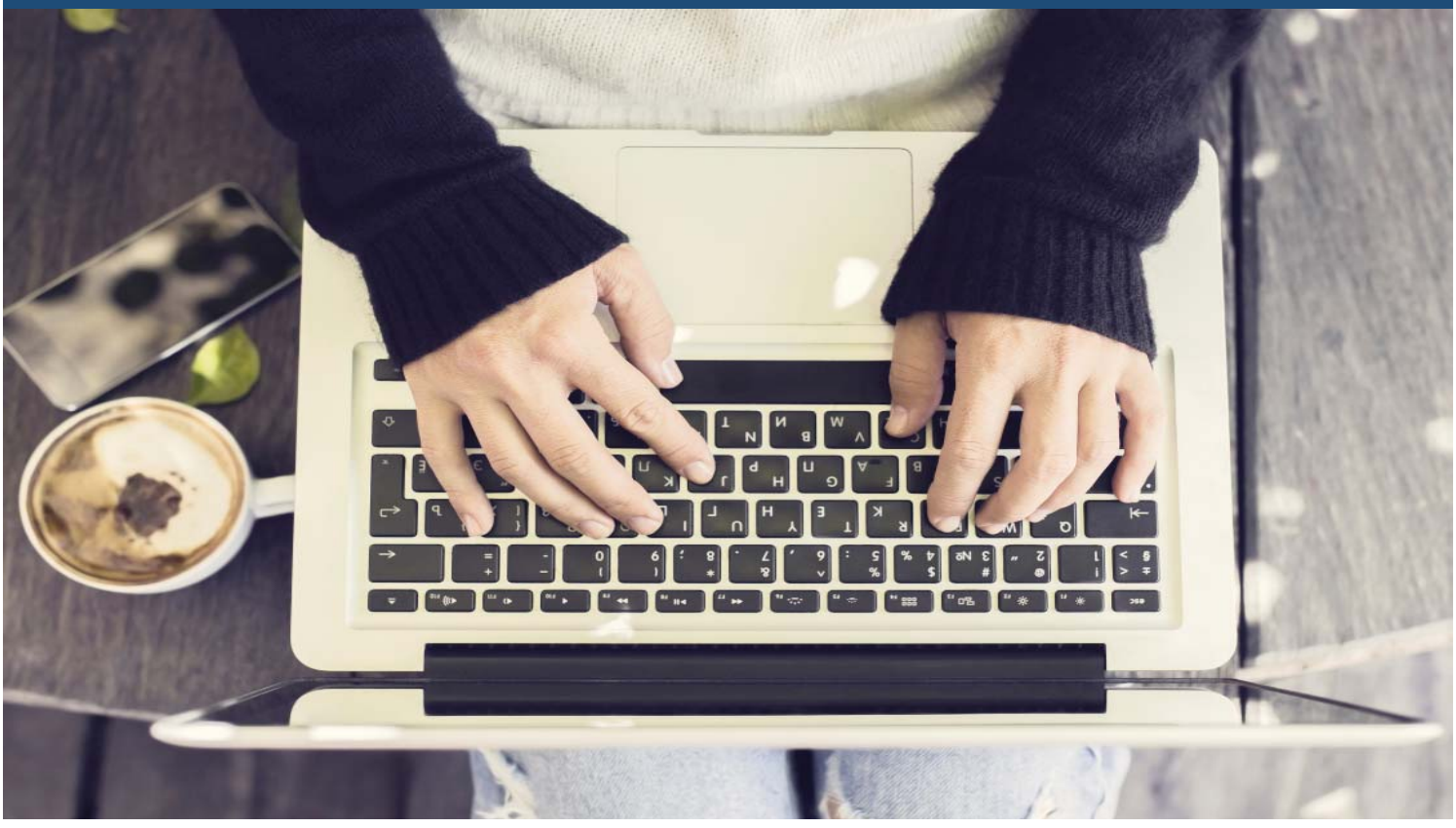


Table of Contents

ABOUT THE AUTHOR

Amelia Vance is director of education data and technology at NASBE.

Policymaking on Education Data Privacy: Lessons Learned

By Amelia Vance

When teachers and schools use data and technology to tailor instruction to individual needs, students benefit through enriched, accelerated learning. Teachers and schools can use education data to measure whether particular teaching methods are promoting student learning. State policymakers can use data to make judgments about the effectiveness of standards implementation and then improve policies or allocate additional state funds or technology support in response. Parents can have timely information about whether their child is on track to graduate ready for college or a career and how their school compares with others in the state.

Protecting student data privacy is at the core of effective data use. Unfortunately, the data that schools use to improve instruction are not always adequately protected, and they are often disconnected, decentralized, or aggregated in a way that leaves the information vulnerable to attack. This vulnerability sparked a growing pushback against the use of data in schools.

In 2015, 187 bills in 48 states were introduced on the topic, up from 110 in 2014. Since 2013, 34 states have passed new laws on student data privacy; an even larger number of states created new policies or regulations on this topic (see map 1). While states have clearly recognized the urgent need to act, many of the bills and policies unintentionally restrict educational technology use and innovation.

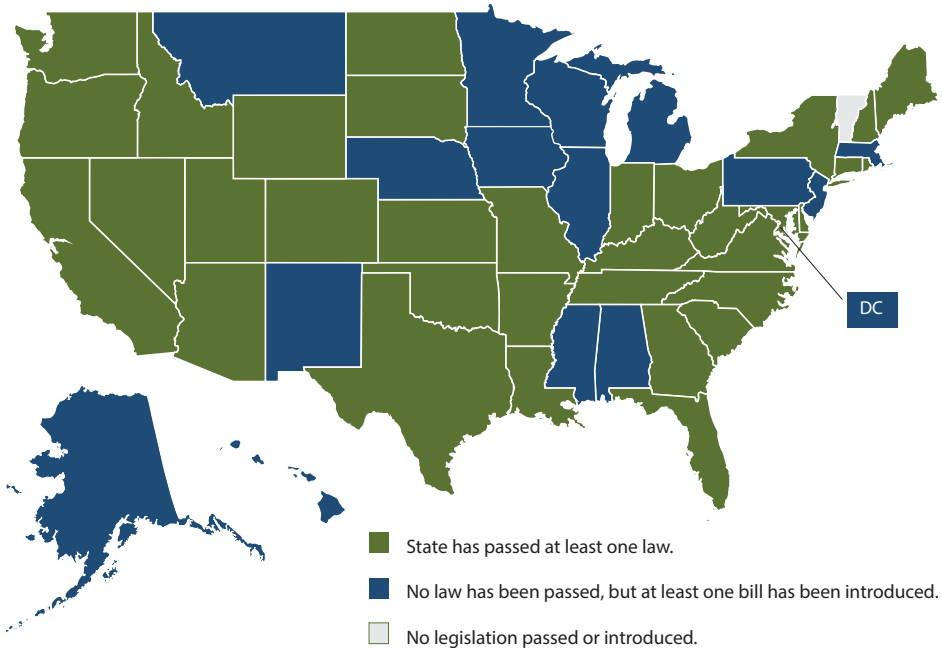
State boards of education (SBEs) are major players on education data privacy: In 36 states, the state board has at least some authority over education data privacy, and states continue to consider expanding those powers. In doing so, many state legislators recognized that SBEs are well placed to protect student privacy. Boards can work directly with parents and educators by holding public hearings and creating committees, and they can respond quickly to changing technologies by developing regulations, guidance, and best practices.

Just as education data privacy was emerging as a hot topic in 2013, state boards sought assistance in understanding the issue. In mid-2014, the National Association of State Boards of Education (NASBE) launched a major effort to help SBE members address issues around data privacy. NASBE's goal has been to ensure that state policies protect student privacy while enabling the critical improvements in education that come from the use of data to personalize learning and support equitable opportunities for all students.

Over the past two years, NASBE provided technical assistance to policymakers in 5 states, held education data privacy meetings attended by representatives from over 30 states, published analyses on student data privacy, participated on panels, and joined coalitions representing key parties working in the student data privacy space. In addition, I have spoken with nearly every state education agency on this topic and gathered every state law and regulation that deals with education data privacy, as well as many state policies and guidance, in order to prepare analyses, conduct policy audits, and identify gaps in a state's education privacy landscape.

This work has yielded key lessons that should be shared with all policymakers interested in education data privacy. In particular, SBEs have been given many powers that—if exercised—could promote an essential balance between

Map 1: 34 States Have Passed 53 Laws Since 2013



protection of privacy and effective use of data and technology in education. My hope is that the knowledge gained during this recent cycle of rapid and vigorous policymaking can be used to create the best possible education data privacy regime across the country.

LESSON 1

State Boards Shape Data Privacy Policy Significantly.

As education leaders and policymakers, SBEs have a responsibility to ensure that state and local data collection is secure and protects individual rights. SBEs should take action if state policy falls short of these criteria for effectiveness. They have a further responsibility to use their state platforms to call for changes in federal law and industry standards that would ensure appropriate collection, use, and security of education data.

State boards are well positioned to act. As noted above, 36 already have some legal authority over student data privacy, and that authority is growing. Since 2013 28 states have introduced bills that would put SBEs in charge of some aspect of student data privacy, with 14 of those bills passing into law.

These laws give SBEs a variety of responsibilities, ranging from ensuring compliance to shaping data privacy policy (see box 1). Sometimes the legislature specifically gives the state board the task of writing the state's educational data collection policy. In some states, this is a general requirement. For example, Nebraska's law requires the state board to write binding rules, interpreted just like a law, for data sharing.[1] In other states, the board gets detailed direction on fulfilling this task. In West Virginia, the legislature spelled out a long list of criteria for all data-sharing relationships with research organizations.[2] In New Jersey, the statute tasks the SBE with creating regulations that will protect the right of students and parents to have access to student information, protect their right to privacy, and protect "the opportunity for the public schools to have the data necessary to provide a thorough and efficient educational system for all pupils."[3] Other state boards have acted independently, using their authority as overseers of education in their state, to pass important data privacy reforms (see box 2).

Transparency has increased as a result of elevated state board roles in education data privacy. One of the main reasons state boards began to be named as the primary state policymakers in this arena was the fact they operate openly (see box 3). Unlike the operations of state education agencies (SEAs), meetings of the state board are public and frequently covered by the media. Before state boards gained their current responsibilities in data privacy, many states handled student data primarily within SEAs and without public process or scrutiny, according to Oklahoma State Representative Jason Nelson, coauthor of one of the first state student privacy laws passed in 2013. Nelson says this was a major factor in Oklahoma's decision to give this power to the state board.[4]

However, one of the most interesting and novel responsibilities granted to state boards under recently passed privacy laws goes beyond rule writing. In five states, state boards have been given the authority to supersede aspects of student data privacy laws on a case-by-case basis that must be reported to the public annually.

This authority has only rarely been invoked, but it can help avoid the unintended consequences that frequently accompany new legislation. For example, in Oklahoma, a problematic regulation accidentally banned the release of graduation rates in 54 percent of its districts. Under Oklahoma law, this regulation could not have been fixed by the legislature until mid-2016. Yet because of the law's countermand clause, the state board could intervene to authorize the release of these graduation rates on a one-time basis.[5]

These clauses are subject to public scrutiny through annual reports that are to be delivered either to the governor or state legislature. In them, the state board must list exemptions granted and the reasons for those exemptions.

Lesson Learned. Many state boards now have broad powers under new state laws, frequently because of their public, transparent nature. SBEs can and should use the authority of their office with their newfound legal powers to support purposeful, secure collection and use of education data.

LESSON 2

Stating the Value of Data Is Essential.

"Why do you need my child's data?" This question has underpinned the vast majority of parental concerns surrounding student data privacy. Schools, districts, and states have not always done a good job explaining to parents the vital role data play in education, and this lack of communication has frayed the trust between parents and schools. Even as state policymakers, who rely on these data to make evidence-based decisions, have begun to enact student privacy protections across the country, this question has often gone unanswered. While the majority of the new laws do protect student data, they often don't clarify why the data are needed in the first place.

Better data increase the efficiency and effectiveness of teaching and learning.

[BOX 1]

In 25 States SBEs Write Data Collection Policy

Twenty-five state boards have this duty: Alabama, Alaska, Arizona, Arkansas, Colorado, Florida, Georgia, Idaho, Illinois, Iowa, Kansas, Massachusetts, Missouri, Nebraska, Nevada, New Jersey, North Carolina, Ohio, Oklahoma, Oregon, Tennessee, Utah, Vermont, Virginia, and West Virginia.

In 2014, data on Delaware students revealed that a significant number were college ready but had not or did not intend to apply for college. The state worked with the College Board to send informational packets to students on colleges they could attend, and high school guidance counselors followed up with students and parents to help them through the application process. Before this program, only 80 percent of Delaware's college-ready high school students enrolled in college. After data empowered the state to act, 98 percent of those students enroll in college.[6]

However, such revelations and their origin in data often fail to trickle down to parents. As Aimee Guidera, president and CEO of the Data Quality Campaign, pointed out, "The idea of using data in the classroom can be confusing, daunting, and even scary. Because our kids are unique, we want to be sure they are not reduced to numbers in a spreadsheet."[7]

Parents of special education students often understand better than anyone why data are essential. A poignant article by Troy Wheeler, a parent of children with special education needs, explained how an out-of-state move cemented his belief in responsible data use. Wheeler explained that none of his children's records, including test scores, academic placement assessments, and special education data transferred to their new school. Wheeler wrote that his wife spent hours digging through old files and calling their old district to get information copied and sent. Because the education curricula in their new state differed from what Wheeler's children had been learning, the new school didn't have the information needed to place them in the appropriate course levels. It took six weeks before the new school discovered that Wheeler's son was struggling more than he should have been in math, which meant he had to be placed in a different class. As Wheeler put it, "Because no data followed my son, he was left feeling like he was failing amidst the already difficult situation of adapting to new peers and trying to make new friends."[8]

Because approximately 15 percent of families move each year, Wheeler's case is far from an isolated incident.[9] Schools need individual student data to help them address individual student needs, and the data must be sharable so new teachers can help students from day one. Technology and real-time data analysis can tell teachers earlier whether a student is learning and on track to do well. Such proactive efforts allow teachers to help their students without waiting until quarterly grades or parent-teacher conferences require them to determine whether a student is falling behind.[10]

States have adopted a variety of approaches to communicate the value of data to parents. Districts and a few states are creating "data dashboards," which show parents how their child is doing on an ongoing basis. These districts and states are also finding ways to provide parents direct access to data. For example, products such as Edline allow parents to receive daily reports on assignments, homework grades, test scores, and "even the slides and videos used in class."[11]

A key part of communicating about the value of data is also communicating why educational agencies and institutions partner with companies to store, analyze, and protect data. Parents are especially concerned about data collection when the entity collecting their children's data is a for-profit company. A 2014 poll commissioned by Common Sense Media revealed that 90 percent of adults worry about companies' ability to access and use students' personal information.[12]

For most schools, involving private companies is a matter of practicality: They do not have the personnel or technical expertise to build data centers, create learning software or apps, or host servers. "As many Fortune 500 companies holding sensitive banking or health data have determined," writes the Future of Privacy Forum in a recent report, "relying on the security protections of outside companies that can deploy hundreds of staff and first-class security tools can far exceed the capabilities of individual companies. Compared to large businesses, schools have far less funding and technical expertise. Even large school districts are hard pressed to keep up with the continual security alerts, patches, and updates needed to maintain secure systems of their own."[13] It is incumbent on school, district, and state administrators, as well as board members and other policymakers, to make this case to parents. It is a critical step in building parents' trust that schools are using data for good purposes while they are also protecting student privacy.

Lesson Learned: A vital part of student data privacy policy is explaining to parents why data are collected and how they are used. If parents do not understand how data can help their children, they will not care how the state is protecting the privacy or security of that data. Instead, they may demand that the data not be collected at

[BOX 2]

Alabama Board Takes the Lead

In Alabama, the state board passed a resolution in 2013 that has served as the primary law on student data privacy. The resolution required SEAs and LEAs to take several important steps: regular training in data security and student privacy laws for individuals with access to student data, creation of an external data request procedure that must go through a data governance committee, and local adoption of a student records governance and use policy. The SEA must periodically audit and monitor district practices and policies.

Source: Alabama State Board of Education, To Approve the Alabama State Board of Education Data Governance Policy, Resolution, Passed October 10, 2013, **http://www.alsde.edu/sites/boe/_bdc/ALSDEBOE/BOE%20-%20Resolutions_3.aspx?ID=2018.**

[BOX 3]

The Question of Directory Information

Transparency is particularly important when discussing directory information, a legal term that describes information that schools can disclose to anyone without parental consent. Called directory information because it is information that would typically be included in a school directory, it can include a student's and parents' names, address, telephone number, e-mail address, date and place of birth, honors and awards, clubs a student participates in, and dates of attendance. It could also include a student's biography in a drama playbill, an honor roll list, the yearbook, or a sports activity list that includes heights and weights of team members.

Schools must annually notify parents about what they consider directory information. Directory information is the only category of data collection under FERPA for which parents can opt their children out of collection or disclosure.

Some privacy advocates argue that more parents should be opting out of release of directory information. "Directory information may sound innocuous, but it can include sensitive information about each student that is quite detailed," said Pam Dixon, executive director of the World Privacy Forum, "And after the school releases this data, it is considered to be public information, and you've lost control of it. I don't think most parents know this."[a]

"Parents are worried about information held by vendors," said Sheila Kaplan, who helped draft New York's student privacy law. "Yet it is the schools that are selling the information or sharing it and allowing it to be sold. And schools should not be data brokers." Kaplan's organization, Education New York, has published a model state bill that restricts schools sharing of directory information.[b]

Data Quality Campaign's Paige Kowalski suggests an additional way of protecting directory information: Require enhanced transparency about what directory information schools disclose by requiring that the annual notice to parents include a disclosure of those to whom schools have disclosed directory information in the past year. "To help parents make informed decisions, schools must be more transparent about what data is shared and how they're making these decisions," Kowalski said.[c]

a. Herb Weisbaum, "Privacy Quiz: How Do You Stop Schools from Sharing Kids' Data?" NBC News, September 8, 2015, **http://www.nbcnews.com/business/consumer/student-privacy-n423466**.

b. Sheila Kaplan, interview with author, March 18, 2016; Education New York, Model State Law: Student Privacy Protection Act, accessed March 18, 2016, **http://educationnewyork.com/files/Model State Law 1.pdf**.

c. Interview with author, March 18, 2016.

all. SBEs and other policymakers can use their bully pulpits to explain the value of student data to parents and other members of the public.

LESSON 3

More Transparency = More Trust

Building parents' support for quality data care and use is not possible without transparency about what data are collected. States and districts must clearly convey to families and the public what data are being collected and for what purpose, who gets to see them, and what happens to them once the student leaves the system.[14] In the more than 300 bills addressing student data privacy to reach state legislatures in the past three years, very few require that schools, districts, and the state put forward understandable information for the general public.

A few recently passed state laws have addressed transparency in three key ways: requiring that the SEA create a publicly available list of collected data, occasionally with a description of why it is collected; requiring the SEA or SBE to create and make available policies and procedures used by the state to comply with the Family Educational Rights and Privacy Act (FERPA) and other relevant federal privacy laws; and mandating that the state governor and legislature be notified about potential new data elements and any exceptions to the law granted within the past year.[15]

Yet even documents created in the name of transparency generally are long, technical lists and descriptions of data elements that are difficult for privacy experts, let alone parents, to parse. "The easiest way to find information would be to Google so as to get the links to either the school or state info," said Olga Garcia-Kaplan, a parent who blogs about student data privacy on FERPA|SHERPA. "Unfortunately, most school and board of education websites are difficult to navigate, and the information is either buried deep in a section or is just not there. Parents don't have time to read through unreasonably long and complicated privacy policies to decipher whether their children's information is being handled

responsibly. Parents cannot and should not be privacy auditors, and data inventories and privacy policies should have a concise and easy-to-understand summary of the privacy policies and best practices used to safeguard student data and its use."[16]

Audrey Watters, an education journalist, suggested some ways to improve transparency in a 2014 article. Watters recommended that schools place transparency resources such as contracts, lists of tools, and terms-of-service agreements in an organized, accessible place on the school or district's website. She emphasized the importance of using clear language, avoiding jargon when talking about data and privacy policies, and keeping the information up to date. Most important, she advised, this website ought to provide a way for parents to contact a school or district representative with questions or concerns.

Some states have gone beyond what their state law requires to create a real regime of transparency. The Colorado Department of Education was one of the first states to release fact sheets for parents and other stakeholders on topics such as data use, what Colorado collects, and how those data are protected. The West Virginia State Board of Education held public forums around the state to answer community members' questions on this topic.[17] The Louisiana Department of Education released a thorough but understandable guide laying out Louisiana's plan to protect student privacy. It included easy-to-understand charts, infographics, FAQs, and best practices. The Wisconsin Department of Education's website is easy to read and navigate, and it also provides sections for districts, schools, and parents (see box 4).

A recent task force report from the Aspen Institute describes what is necessary to build the trust necessary for learning, particularly around data-driven education. A key characteristic for a trusting environment is transparency that "enable[s] learners and other stakeholders to clearly understand who is participating, what the norms and protections are, what data is collected and how it is used."[18]

Lesson Learned: States ought to go beyond what is required by most current laws so trust can be established between parents and schools on student data privacy. Because they are already frequently in charge of student privacy work in their state, SBEs can take a leading role in advocating for easy-to-understand information that helps parents and others learn how data are being used and protected. They can also act by example: Most have their own websites. Particularly for state boards that have authority over student data privacy, providing web links and information on student data privacy is key for transparency.

LESSON 4

Early Adopters Can Shape the Second Generation of Laws, and Other States Should Learn from Them.

Most states that passed student data privacy laws in the past two years based their legislation on two models: the Student DATA Act in Oklahoma and the Student Online Personal Information Protection Act (SOPIPA) in California. These two laws were the first of their kind. Oklahoma's law was written and passed in 2013, when student data privacy was major news for the first time. Its governance-focused provisions regulate schools, districts, and the SEA. California's law, by contrast, focuses on the operators of online educational services. Instead of restricting the school's collection of information, SOPIPA and companion bill AB 1584 restrict what companies can do with the information they obtain through their contracts with schools.

Oklahoma's law limits the student data districts can give to the SEA, restricts access to student data, defines circumstances in which data can leave the state, and requires the SEA to develop a data security plan.19 The law charged the state board of education with creating data confidentiality standards for student personally identifiable information and prohibited sharing certain data—including Social Security numbers, religion, political party affiliation, or biometric information—with the state or federal government. Nine other states have passed laws based on Oklahoma's.

SOPIPA, passed in 2014, keeps companies from selling information they gain through their K-12 school software or from using that information to target advertising to a California student or parent, either on the educational website or on another site, service, or application. The companies are also prohibited from using student information "to amass a profile about a K-12 student except in furtherance of K-12 school purposes."[20] The companies may use student information for adaptive learning or any other legitimate school

[BOX 4]

Website Transparency

Most states could improve (or create) websites and thus transparency on student data privacy. A survey of 50 states revealed the following:

- 15 SEAs do not have webpages that address student data privacy.
- 16 websites have information that parents can easily understand.
- 8 have FAQs, 7 have information specifically for schools or districts.
- 6 only have information on FERPA.
- 5 have information that would help with staff training.

Source: Jordan Koch, Survey of SEA Websites on Student Data Privacy, Alexandria, VA, National Association of State Boards of Education, February 27–28, 2016.

purposes and may use deidentified student information to improve or demonstrate their services. The bill went into effect on January 1, 2016. Since then, 10 states have passed laws based on SOPIPA.

The California companion bill, AB 1584, which was introduced and passed in 2014, governed schools' ability to contract with outside vendors. This law requires that all such contracts include provisions specifying that pupil information continues to be the property of the school, guaranteeing that companies will ensure the security and confidentiality of the information, and describing how the school and the vendor will work together to ensure FERPA compliance. Any contract that fails to meet these provisions will be rendered void.

Lesson Learned: The early adopters provide a valuable model for other states. In this case, model legislation in Oklahoma and California was adopted in many states, and even bills not explicitly modeling those laws incorporated many elements from SOPIPA and the Student DATA Act. As the student data privacy discussion continues, SBEs should pay close attention to bills that raise new student privacy issues. For example, the ACLU's model student data privacy omnibus of bills, at least one of which was introduced in nine states in 2016, raises the issue of student privacy on one-to-one devices. Proactive board members and other state policymakers will examine these types of bills to determine whether accidental harms could result and how to minimize them, and they will work to get well-vetted bills through the legislature.

LESSON 5

First Adopters Should Look at Second-Generation Laws and Revisit Existing Legislation

While the Student DATA Act and SOPIPA provided a starting point, many states continue to refine their legislation to address needs of their state's particular educational and policy environment. Georgia, for example, adopted a bill in 2015 that drew on both Student DATA Act and SOPIPA. In addition, the law included provisions on training state, district, and school staff to protect data privacy, added training to the responsibilities of the state chief privacy officer, and included training as part of the state's data security plan. The legislation also expanded and clarified provisions of the original Oklahoma and California laws. Georgia's law has been hailed by many as a new best-practice model.

> "Several states introduced bills that would have rendered most school activities impossible because they placed severe restrictions on what data could be collected and how they could be used."

Combining model laws from other states is just one way states can keep their laws up to date. Some have done this piecemeal. For example, Oklahoma has amended its original law through the legislature a few times since enacting the Student DATA Act. SOPIPA formally became law only in January 2016, and few of the laws based on SOPIPA have been fully implemented, so there has been little chance to improve the law. However, many organizations and companies have already expressed confusion about certain terms in SOPIPA, indicating that there is room for clarification.

For example, SOPIPA banned "targeted advertising" but does not define it, and many districts and companies do not know what it means. This term would most likely apply to advertising for a baseball game that is delivered to a student because they had written an essay about baseball. But beyond those obvious examples, the term's ramifications are uncertain. Many websites and online services—Amazon.com, Khan Academy, MOOC providers, Netflix, or the *New York Times* website—offer "recommendations" after a user reads an article, takes a class, watches a movie, or looks at a book. These recommendations can be useful: A person who enjoyed an online class on the mathematics of juggling might also enjoy a class on probability; a book recommendation could allow discovery of a new author. It is not clear whether the ban on targeted advertising encompasses these "recommendation engines."

Two 2016 bills that appeared likely to pass in Virginia and Utah take different approaches to fixing this issue. Virginia HB 749, awaiting the governor's signature at this writing, amends its SOPIPA-style law to define "targeted advertising," while Utah HB 358 specifically allows vendors to use "recommendation engines" and then defines that term. California and other states that have adopted laws similar to SOPIPA would do well to follow their example.

One great example of a state taking the time to reexamine their laws to ensure the best balance between privacy and good data use is found in a 2015 law passed in Delaware. The Student Data Privacy Protection Act, SB 79, created a task force to study and report on what should be included in a new law that would regulate the data security and privacy responsibilities of the state's SEA. To ensure that a wide range of views are represented, the task force includes representatives from the state board, the SEA, the attorney general's office, the head of the state school board association and school officers association, the PTA, and two industry representatives.[21] Similarly, Maryland has a pending bill that would establish a council to study and make recommendations regarding the development and implementation of the student privacy law they passed in 2015.[22]

Lesson Learned: Laws can and should be improved and enhanced. SBEs would

be wise to use their influence and ability to make new rules to ensure that student privacy laws and regulations are updated so they adequately balance privacy and the use of data in education and so the schools, districts, and SEA personnel who implement them also understand their intent.

LESSON 6

Student Data Privacy Legislation Can Cause Unintended Harms, so States Should Take Care to Clarify Laws or Regulations.

Analyzing the effects of laws and policies in other states can help policymakers craft good data protection plans in their own. Other states' laws sometimes offer cautionary tales of language that proves to be imprecise or implementation issues that were not fully thought through. Frequently, these issues arise when key stakeholders do not get a chance to weigh in on the legislation's potential impact before its drafting.

Words Matter. Legislation on any topic should be carefully drafted and easy to understand, and this principle holds especially true in a complex, fast-moving arena like data and privacy. In 2014, several states introduced bills that would have rendered most school activities impossible because they placed severe restrictions on what data could be collected and how they could be used, even for education purposes. In a few states, these bills passed into laws that will create headaches for courts trying to interpret them and policymakers trying to implement them or introduce new technology-based educational innovations in a way that complies with them. Legislators did not mean to create these problems. But when laws contain ambiguous language or there is confusion about the meaning of provisions, policy will be enacted inconsistently.

In the drafting of legislation or a privacy policy, the specific words used, or not used, make a big difference. For example, the term personally identifiable information means different things in different contexts, and implementing a law that references it will be difficult if it is not defined clearly.

In 2015, New Hampshire passed a law requiring teachers and teacher candidates to get written approval from the school board, parent, and supervising teacher before they can video record themselves in class. New Hampshire school districts must also hold public hearings before video recordings can be made. Teachers and teacher candidates routinely use video recordings to elicit feedback and evaluations from their professors. Many assessments that teachers must take to become certified, such as edTPA, require such recordings.

The vagueness of the New Hampshire law "generated questions for school districts across the state regarding how many public hearings and permission slips are needed for each recording, as well as how school officials should handle situations involving students with disabilities who regularly record classes."[23] The law's sponsor has now written a clarifying amendment that may be passed in 2016, but in the meantime, New Hampshire districts and teachers seeking credentials they need to keep teaching are in chaos.[24]

Laws like these can hamper many great uses of technology in the classroom: teachers' use of Skype to connect their students with children in classrooms around the world, for example, and telepresence robots that allow children who cannot attend school to be remotely present. In one Maryland school, this type of robot allows 10-year-old Peyton, undergoing chemotherapy for liver cancer in New York, to attend classes with her friends. Use of this technology would not be possible if Maryland or other states that support sick children in this manner had similar restrictions on video recording.

> "States should identify who needs to be at the table as they prepare to make decisions; all can help ensure that policies are comprehensive and have wide support."

Neither is federal legislation immune to the problem of unintended consequences. A bill that Representatives Kline, Scott, Rokita, and Fudge introduced before the US House of Representatives in 2015 allows for student data to be shared with education researchers so educational agencies can determine, for example, whether students are learning what they need to know in high school in order to succeed in college. However, the provision states that research cannot be conducted, even if the school needs it, if it is not designed to improve the instruction or testing of students attending that school. This approach could restrict studies, for example, that deal with teachers only, or studies where a group of students who are not using a particular method are a control group in a research study. The language would also prevent the use of valuable past data to support future improvements to teaching and learning.

Privacy Problems with Privacy Legislation. In 2014, Senators Ed Markey (D-MA) and Orrin Hatch (R-UT) introduced a bill in the US Senate that would have amended FERPA. The bill clarified the right of parents to access and amend their children's education records, whether they are held by an educational agency or an outside contractor. To facilitate that access, the bill stated that school districts must maintain a record of all outside parties that receive student information and describe the information shared with them, which FERPA already required (though not as explicitly). The bill language explained that parents must

[BOX 5]

Kansas Sees Unintended Consequence

When Kansas lawmakers passed a student privacy law in 2014, district stakeholders were not consulted. The law required schools to get parental permission before students could be surveyed on certain sensitive topics, and it did not provide an exception for surveys in which respondents were anonymous. Kansas conducts an annual survey in which students anonymously respond to questions about risky behaviors such as drug or alcohol use. The survey helps nonprofits and districts target support to schools with high incidences of reported risky behavior. As a result, districts projected that parents would not return sufficient numbers of permission slips and that the number of children taking the survey in 2015 would drop to 25,000, compared with 100,000 who took the survey in 2014.

Source: Mike Hendricks, "Unintended Consequences Cripple Kansas School Surveys of Student Use of Drugs, Alcohol," *Kansas City Star*, January 6, 2015.

be given access to personally identifiable information about their children that is held by an outside party to the same extent and in the same manner as the state education agency.[25] At a minimum, this provision would have meant that each company needed to create files on individual students (although student data may have previously been collected only in the aggregate). The bill would also have forced companies to collect personal information about parents so the company could verify the identity of anyone asking for an individual child's data. As the Data Quality Campaign noted after the bill was introduced, it makes more sense to ensure that schools, not companies, are keeping track of the information they share with companies so that parents can obtain files on their children directly from the school.[26] Clearly, these consequences would have been contrary to the intent of the bill's authors.

Another bill, introduced in Congress by Senator David Vitter (R-LA) in 2015, placed parental consent at the heart of its student data privacy framework. The bill would require parental consent for any third-party access to student data. However, a requirement that parents opt in every time a classroom uses a new technology or each time their child's data are shared prevents schools from using data in positive ways. The requirement in the Vitter bill could mean that parents would need permission slips every time their child's school adds new education software or each time a new bus driver needs a child's address. According to many privacy experts, parental consent can be appropriate in some circumstances, but not when it comes to core academic activities. The bill gives the illusion of transparency but would likely overwhelm parents with permission slips and make timely and effective implementation impossible. Schools may be left having to keep some student records on paper and other on computer systems, increasing the likelihood that they will simply lose track of some students.

The approach this bill takes could also create major equity imbalances. In Louisiana, which required parental consent for data sharing in a 2014 law, schools had trouble getting parental consent for data sharing, such as nominating children for college scholarships.[27] Therefore, children whose parents missed or ignored the schools' requests could not be nominated.

A better approach is to give parents a role in protecting their children's data while letting schools use valuable technology to help kids succeed. For example, Senators Blumenthal and Daines introduced a 2015 bill that allows schools to grant consent on parents' behalf as long as they do so in compliance with FERPA—for example, by mandating that schools must share all of the data collected about a student with their parents upon request.

Privacy is important, and states and the federal government can protect it without inadvertently banning the use of data and technologies that aid children and prepare them to compete in the global economy.

The Need for Input. Many state bills introduced over the past two years did not give district stakeholders—from classroom teachers to chief technology officers to superintendents—an opportunity to weigh in on how the bills would affect educational work. This oversight created problems in a few states (see box 5). Louisiana districts, unsure of the implications of the student data privacy law the legislature passed in 2014, took an extremely conservative view about what information could be released: School administrators worried about showing football players' names on the big screen during games, having a yearbook, and even whether they could hang student artwork in the hallways.[28]

The law was amended in 2015 to give districts more discretion. However, districts had already spent countless hours complying with the law, going as far as sending teachers on home visits to get permission forms signed.[29] If legislators had met with district staff before the law's passage in 2014, this unintended consequence could have been avoided.

Biometric data are commonly used as an authentication mechanism in which a physical characteristic is measured or compared against stored information—for

example, scanning a fingerprint or using facial recognition. However, some have defined it more broadly to incorporate any stored data on physical characteristics that might be used in school, such as T-shirt sizes. Several state laws passed in 2014 and 2015 restricted biometric information collection but didn't define the term.

Other states banned biometric data collection outright. In Florida, a 2014 law banning such collections ended up requiring several school districts that had invested substantial amounts to install biometric scanners for school lunch lines to disassemble those machines. Legislators were primarily motivated by the "creepy factor"—how people felt when hearing a description of the technologies—and failed to weigh testimony about the positive uses of biometric technologies occurring in schools across the state.

States should identify who needs to be at the table as they prepare to make decisions about privacy laws and policies. Parent voices are an essential part of this process, but so are teachers, principals, administrators, chief technology officers, vendors, lawyers, and state leaders. All can help ensure that policies are comprehensive and have wide support across the state.

After examining existing laws and policies, the state should examine its infrastructure to see if it securely stores and analyzes data. For example, Colorado's legislature and state board of education commissioned a review in 2007 to determine whether its existing data storage and analysis structures were adequate. The board specifically asked about the ease of collecting data, the hardware and software in use at state and local levels, and the ability of districts to share data with one another and with the state education agency.[30]

> "While state legislatures need to act to fully fix a law that has produced many unintended consequences, the state board can mitigate those consequences in the short run."

Another problematic provision of the Kline, Scott, Rokita, and Fudge bill deals with the security safeguards, and it also illustrates the importance of running legislative language past schools, districts, and other stakeholders. Security safeguards are essential: Schools and service providers must establish them to prevent malicious actors from gaining unauthorized access or disclosures. Without those safeguards, even the strongest privacy protections could be for naught. The Kline bill, however, gave schools and local and state education agencies the responsibility for ensuring that the third parties with which they contract have adequate information security practices. This presents an insurmountable burden for almost all schools, since they simply do not have the expertise or resources to assess third parties' practices or determine whether they are complying with industry security standards. Requiring schools rather than third parties to fulfill this requirement thus virtually guarantees noncompliance. If schools and districts had been consulted, the bill might instead have given vendors responsibility for legally certifying that their security meets industry standards or included another provision to take the burden off schools or districts, which lack the expertise to certify security.

Asking those who have to implement laws how they would affect their districts or schools is one of the best ways to avoid such accidents in Congress and state houses. Unless such consultations take place, new student privacy laws will likely end up harming students more than they protect them.

Policymakers should also discuss potential laws or rules with people working in industry. Protections that seem reasonable to laypeople may strike someone with technical expertise as unimplementable. Data privacy inherently involves technology, so it is vital to have someone familiar with technology—and in the myriad forms likely to exist across districts—providing input on all decisions. Such input could waylay, for example, a law that one state considered to require that data "in the cloud" be segregated by school—technologically impractical and cost prohibitive.

Industry may also be able to help keep laws within their intended confines. For example, such input could have prevented the case in which a Louisiana parish decided to forgo creating a yearbook because staff believed a 2014 state law required written consent of each parent in order to include each child in the yearbook.

Many states have decided to require "comprehensive security" for all vendors, with no differentiation between those that handle sensitive information such as health records and those whose software contains aggregated "here's how well this student played this game" information, which wouldn't need a similarly high level of security. Some state and district contracts ban the use of a "portable media device" to store or transmit student personally identifiable information. But since a camera is technically a portable media device and pictures are "personally identifiable," such a ban could encompass things like school pictures or at a minimum require that a school or district revise policies to clarify that taking school pictures is acceptable.

Obviously, state legislators do not intend to ban school pictures or restrict student access to technologies that could help them learn better or teacher access to software that helps identify students who need extra help. By inviting companies to the table, states can avoid

accidentally doing these things.

Fear-Based Policies. Fear drives some bills' drafting but typically fails to produce the best legislation. Such laws will likely need fixing down the road. The Vitter bill, for example, forbids funds from being spent to collect data measuring "any type of psychological parameter" and then fails to define "psychological parameters," opening the door for uneven, confused, and retrogressive interpretations. Left undefined, this aspect of the legislation could be understood to ban almost all tests or quizzes because they score student knowledge—a psychological parameter. Though the provisions of this bill on psychological data collection reflect real stakeholder concerns, the ban is so widely targeted and loosely written that it would likely cause more confusion and harm than good.

The bill could also ban college and career counseling given to students by forbidding "any effort to obligate an elementary school or secondary school student to involuntarily select a career, career interest, employment goals, or related job training." Many students rely upon their counselors' input to not only suggest possible college and career options but also to help guide them through complex applications processes for postsecondary education and employment opportunities. Whatever modest privacy gains might be made if the bill became law are bound to be outweighed by the losses in student college and career readiness that would follow.

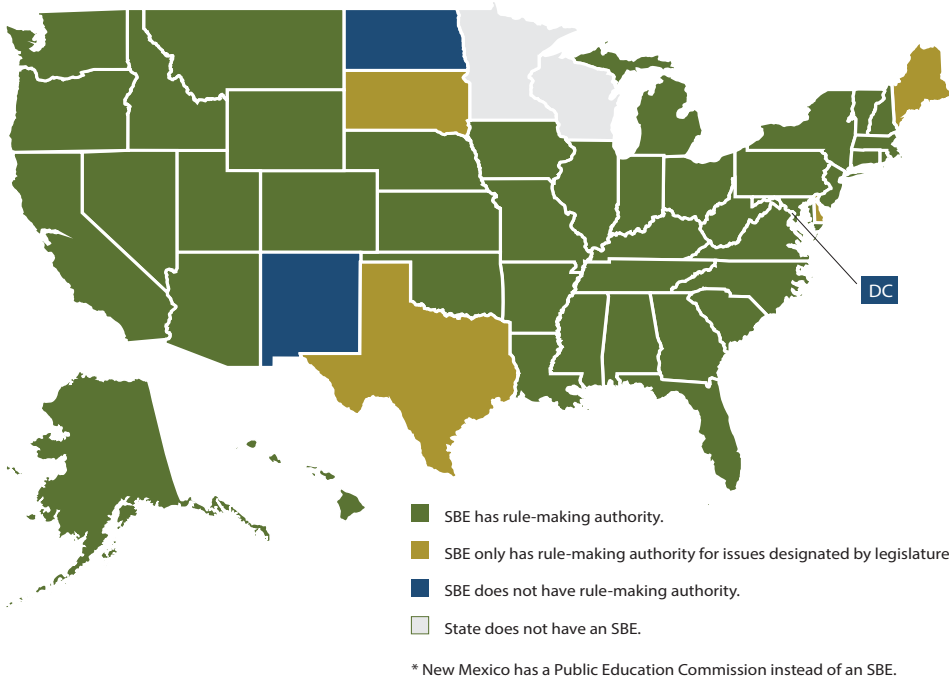
Finally, the bill stipulates that education records be destroyed any time a student leaves any educational institution. These conditions are simply too broad: Records would be automatically destroyed for transfer students and even students moving between schooling levels, impairing the continuity of learning during transition periods. This provision could be especially harmful for transient families, such as the children of parents in the military. The data deletion requirements would also harm students forced to leave their education system because of extenuating circumstances. If these students were to attempt to finish their education, they would return to find their records had been destroyed.

It is vital to strike a balance between privacy and effective use of student data and education technology. Most states have passed laws that create real solutions, rather than reactionary rules guided by fear. For example, many states have created a governance structure for schools, districts, and states, or they directly regulate companies' actions. State policymakers should steer clear of legislating fear-based policies.

Lesson Learned: It is essential for all data privacy legislation to be vetted with a fine-toothed comb for vague language that may unnecessarily restrict the positive use of data. SBEs are ideally placed to fix these problems: 45 have rule-making authority, and many have received additional authority from recent state student privacy laws. Consequently, some state boards can pass binding rules, which essentially work just like law. Such rules can spell out guidance on problematic student data privacy laws. While state legislatures need to act to fully fix a law that has produced many unintended consequences, the state board can mitigate those consequences in the short run and give clarifying guidance to state education agencies, districts, and schools guidance (see map 2).

State boards can also call for proper review of legislation to forestall unintended consequences as legislation is being considered, using their platform as public officials. They also can convene stakeholders to ensure their voices are included in the law- and rule-making process.

Map 2: SBE Rule-Making Authority



* New Mexico has a Public Education Commission instead of an SBE.

LESSON 7

Human Error Is the Biggest Factor in Privacy Violations, so Training Is Essential.

According to IBM's 2014 Cyber Security Intelligence Index, human error is a factor in 95 percent of all data security incidents.[31] Many are avoidable mistakes that could be minimized with training and oversight. All staff should be made aware of the importance of creating passwords that are not easy to guess, double-checking emails when sending attachments to ensure that the right data

are sent, detecting whether an email has a potentially malicious link, and knowing what to do if a device with sensitive information is lost.

Such training can prevent major data breaches, such as the one that occurred in Chicago in 2013, which resulted in the names, birthdates, gender, ID numbers, and exam information of 2,000 students being accidentally posted online.[32] NASBE's 2014 Public Education Position on student data privacy recognized this need. It noted the importance of states creating a plan to ensure "educators and administrators have the knowledge, skills, and support to use education data effectively and securely."

Anyone who handles data should know how to protect those data. They also need a thorough understanding of how to use data—and how not to. Bill Fitzgerald, privacy initiative director at Common Sense Media, cited a privacy violation that exemplifies the need for such training: A school principal posted a question about a student-related issue on a vendor's website, disclosing the student's first and last name in order to elicit information from the vendor. Worse, the vendor replied on a publicly accessible webpage. The principal and the vendor's staff would have benefited from training on privacy laws and thus would have learned "the implications of sharing student information, including information about behavioral issues, on the open web," Fitzgerald said.[33]

All district and school staff need such training. Most people press "yes" when they download an app to their tablets without reading the terms of service. However, when teachers are downloading that app to students' tablets, they must know what information that app is collecting and how that information will be used, stored, and shared. Teachers can learn to recognize potential privacy hazards and when they need to talk to an administrator to see if a particular app is safe to use. Districts should also decide what level of authority teachers have to make these agreements on behalf of the schools and ensure teachers are aware of the policies.

> "Although more than 300 bills have been introduced over the past two years on student data privacy, few mention training."

Although more than 300 bills have been introduced over the past two years on student data privacy, few mention training. Paige Kowalski, vice president of policy and advocacy at the Data Quality Campaign, noted that it will be difficult for districts and educators to implement new state laws with fidelity without training, especially considering the large number of new roles and responsibilities districts are expected to take on under those laws.[34]

Despite the lack of a training requirement in state laws, many states are nonetheless beginning to take action. Maryland and Virginia have policies requiring comprehensive privacy training for education personnel. Similarly, Colorado requires new SEA employees to participate in an annual information security and privacy fundamentals training in order to retain access to the department's network.[35] Wisconsin's public training module offers a lesson followed by a quiz on student data privacy on the SEA's website.[36] Some school districts, such as the Cupertino Union school system in California, offer a preapproved list of websites, apps, and other tools that teachers access in coordination with data privacy training.[37] West Virginia's SEA will review vendor contracts with districts to help ensure that the contract's privacy and security safeguards are adequate.

Regardless of the approach, training is essential. The Privacy Rights Clearinghouse (PRC) tracks data breaches across the United States. As of February 23, 2016, the PRC Chronology of Data Breaches documented 767 breaches that involved educational institutions and were made public between 2005 and 2016. These incidents involved nearly 15 million breached records.[38] Of those breaches, 221 occurred because someone accidentally posted sensitive information on a website, mishandled information, or sent sensitive information to the wrong party. Those 221 do not include the multiple breaches that occurred due to other types of human error: a teacher not locking their computer at lunch, an administrator clicking on spyware or malware, or a flash drive falling out of someone's pocket at a restaurant.

Lesson Learned: Policymakers must ensure that each state has training laws and policies and identify resources to make training feasible. Especially in the states where state boards have rule-making authority, they can set training policies themselves or can mandate or recommend that each district create an education data privacy training plan. Many state boards also have authority over teacher preparation standards and administrator training and can require or strongly suggest that administrator and teacher preparation colleges cover this topic. "Even though the odds of an earthquake are low, teachers in California are trained how to keep students safe." said Kowalski, "Why do we continue to risk student safety by not also training teachers how to deal with the far more regular occurrences of privacy and confidentiality breaches?"

CONCLUSION

State boards of education have significant legal authority over education data privacy. They should use it. Many already have flexed this authority. In states such as Alabama, Utah, and West Virginia, the state board of education serves as the primary leader on education data privacy, providing the laws and guidance

necessary to ensure a balance between protecting student data and allowing the vital use of data and technology in education. State boards in Oklahoma and Idaho have used their "override" authority to provide one-time authorization to fix accidental consequences discovered in their student privacy laws and regulations. Other state boards provide feedback on student privacy committees, write rules and guidance for districts, and hold public meetings around their state to answer questions.

In addition to the newfound legal authority many state boards enjoy, board members can use the bully pulpit inherent in their positions as public officials in open meetings, pushing for improved transparency, training, and reviews of draft legislation to ensure that privacy laws thoughtfully protect students but do not accidentally hinder student learning and success.

In the course of making new laws and implementing them, states have discovered both pitfalls and best practices, and they will continue to do so. Laws creating a governance structure for schools, districts, and SEAs have been widely adopted across the country, as have industry-focused laws. States, like Wisconsin, that have put a premium on transparency have found increased trust from the public and have passed fewer potentially problematic laws. No law is perfect, but, in avoiding writing laws or rules in a vacuum, states can avoid writing laws or rules in a vacuum by ensuring that the people on the ground who must implement those laws are involved in the drafting process. Expert input on congressional bills can lead to stronger privacy protections that still leave room for student learning and school improvement.

State boards that have not weighed in on privacy should. Data privacy will be ever more important as education becomes more personalized and dependent on technology. In the first two months of 2016 alone, new privacy issues related to one-to-one devices and the surveillance of students in school have led to a model bill crafted by the American Civil Liberties Union that has been introduced in four states. Seven student privacy bills are pending in Congress, and two of those are may pass over the next two years: a rewrite of FERPA and an industry-focused bill that would have significant effects on educational institutions.

State boards should not wait for a front-page news story about risks to student data, or worse, an actual breach that occurred in their state because someone was not trained to protect student data. States' decisions on privacy could dramatically affect education and student lives for the next decade. By taking advantage of the current spotlight on privacy and using it to make positive changes that balance privacy and good data use, state boards can improve education and create a system where the appropriate use of data can help all children succeed.

NOTES

1. R.R.S. Neb. § 79-2,104.

2. W. Va. Code § 18B-1D-10.

3. N.J. Stat. § 18A:36-19.

4. Jason Nelson, "Oklahoma's New Student DATA Act Sets Guidelines, Protections," *The Flashlight* (blog), September 26, 2013, **http://dataqualitycampaign.org/blog/2013/09/oklahomas-new-student-data-act-sets-guidelines-protections/**.

5. Nate Robson, "State Education Board Votes to Allow Data Release," *Oklahoma Watch*, Aug. 31, 2015, **http://oklahomawatch.org/2015/08/31/state-education-board-votes-to-allow-data-release/**.

6. David Leonhardt, "A Case Study in Lifting College Attendance," *The New York Times*, June 10, 2014.

7. Aimee Rogstad Guidera, "Teachers and Parents Need to Support Their Kids' Learning," *HuffPost Education* (blog), April 29, 2015, **http://www.huffingtonpost.com/aimee-rogstad-guidera/teachers-and-parents-need_b_6771608.html**.

8. Troy Wheeler, "The Impact of Student Data (or Lack Thereof): A Parent's Perspective on the Power It Holds," Ed-Fi Alliance (blog), June 12, 2004, **http://www.ed-fi.org/blog/2014/06/impact-student-data-lack-thereof-parents-perspective-power-holds/**.

9. Tim Henderson, "Americans Are on the Move—Again," The Pew Charitable Trusts (blog), June 25, 2015, **http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/6/25/americans-are-on-the-move-again**.

10. Jose Ferreira, "The Mathematics of Effectiveness," Knewton (blog), April 17, 2014, **https://www.knewton.com/resources/blog/ceo-jose-ferreira/big-data-mathematics/**.

11. Stephen Balkam, "Learning the Lessons of the inBloom Failure," *The Huffington Post* (blog), April 24, 2014, **http://www.huffingtonpost.com/stephen-balkam/learning-the-lessons-of-t_b_5208724.html**.

12. "National Poll Commissioned by Common Sense Media Reveals Deep Concern for How Students' Personal Information Is Collected, Used, and Shared," Common Sense Media, January 22, 2014, **https://www.commonsensemedia.org/about-us/news/press-releases/national-poll-commissioned-by-common-sense-media-reveals-deep-concern**.

13. Joseph Jerome and Jules Polonetsky, "Student Data: Trust, Transparency and the Role of Consent," Future of Privacy Forum, October 2014, **https://fpf.org/wp-content/uploads/FPF_Education_Consent_StudentData_Oct2014.pdf**.

14. Aimee Rogstad Guidera, "Privacy and Trust: The Keys to Effective Data Use," *The Huffington Post* (blog), January 28, 2014, **http://www.huffingtonpost.com/aimee-rogstad-guidera/privacy-and-trust_b_4673864.html**.

15. Student Data Accessibility, Transparency and Accountability Act of 2013, OK. ENR. H.B. No. 1989 (passed May 29, 2013).

16. Olga Garcia-Kaplan, e-mail message to NASBE, March 2, 2016.

17. Amelia Vance, "West Virginia's Steady Course on Student Data," presentation, SXSWedu, Austin, TX, March 9-12, 2015.

18. Aspen Institute, Task Force on Learning and the Internet, "Learner at the Center of a Networked World," (2014), **http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/Learner-at-the-Center-of-a-Networked-World.pdf**.

19. Ok. Stat. 70 § 3-168.

20. Ca. Code 22.2 § 22584-22585.

21. De. Code 14 § 4111.

22. An Act Concerning Education – Student Data Privacy Council, MD. H.B. 430 (2016).

23. Paul Feely, "New Hampshire Schools Review Policy on Video Cameras in Classrooms," *The New Hampshire Union Leader*, December 14, 2015, **http://www.centerdigitaled.com/k-12/New-Hampshire-Schools-Review-Policy-on-Video-Cameras-in-Classrooms.html.**

24. "Student Data Privacy," last modified October 23, 2015, accessed March 11, 2016, **http://education.nh.gov/standards/documents/privacy.pdf**.

25. Protecting Student Privacy Act of 2014, S. 2690, 113th Cong. (2014).

26. Kristin Yochum, "Protecting Student Privacy Act of 2014," *Flashlight* (blog), May 16, 2014, **http://dataqualitycampaign.org/blog/2014/05/discussion-protecting-student-privacy-act-of-2014/**.

27. Corinne Lestch, "Louisiana Schools Struggle with Strict Privacy Law," March 2, 2015, **http://statescoop.com/louisiana-schools-struggle-with-strict-privacy-law/**.

28. Ibid.

29. Ibid.

30. An Act Concerning a Comprehensive Review of the State's Educational Data Infrastructure, and Making an Appropriation Therefore, CO. H.R. 07-1270, (passed June 1, 2007).

31. Fran Howarth, "The Role of Human Error in Successful Security Attacks," September 2, 2014, **https://www.securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/**.

32. Adam Greenberg, "Info on Thousands of Chicago Students Posted to City Website," *SC Magazine* (blog), December 6, 2013, **https://www.scmagazine.com/info-on-thousands-of-chicago-students-posted-to-city-website/article/324470/**.

33. Bill Fitzgerald, "Privacy Protection and Human Error," Common Sense Media (blog), November 4, 2015, **https://www.commonsensemedia.org/kids-action/blog/privacy-protection-and-human-error**.

34. Robin L. Flanigan, "Why K-12 Data-Privacy Training Needs to Improve," *Education Week*, October 19, 2015, **http://www.edweek.org/ew/articles/2015/10/21/why-k-12-data-privacy-training-needs-to-improve.html**.

35. "Maryland Longitudinal Data System Annual Report December 2012," last modified December 12, 2012, accessed March 11, 2016, **https://mldscenter.maryland.gov/egov/publications/MLDSC_Annual_Reports_2012.pdf**; "Information Security and Privacy Policy," last modified March 2014, accessed March 11, 2016, **https://www.cde.state.co.us/cdereval/cdeinformationsecurityandprivacypolicy**.

36. "Student Data Privacy Training," accessed March 11, 2016, **http://dpi.wi.gov/wise/data-privacy/training**.

37. Flanigan, "Why K-12 Data-Privacy Training Needs to Improve."

38. Joanna Lyn Grama, "Just in Time Research: Data Breaches in Higher Education," last modified May 20, 2014, accessed March 11, 2016, **https://net.educause.edu/ir/library/pdf/ECP1402.pdf**.

NASBE | National Association of State Boards of Education

333 John Carlyle Street, Suite 530
Alexandria, VA 22314

The National Association of State Boards of Education represents America's state and territorial boards of education. Our principal objectives are to strengthen state leadership in education policymaking, advocate equality of access to educational opportunity, promote excellence in the education of all students, and ensure responsible lay governance of education.
Learn more at www.nasbe.org.