Student Data Privacy Legislation

A Summary of 2016 State Legislation

SEPTEMBER 2016

EXECUTIVE SUMMARY

Student data privacy was a priority issue in state legislatures in 2016, though as expected, states passed fewer student data privacy bills into law than they did in 2014 and 2015. The privacy conversation has evolved since 2014, and now states have the ability to borrow from each other: California's 2014 Student Online Personal Information Protection Act (SOPIPA), the first to legislate the permissible activities of online school service providers in the digital age, served as a model for many states this session. Most of the states that passed new laws in 2016 had already passed a student data privacy law, a sign that states are building on prior efforts.

Since 2013

- 49 states and the District of Columbia have introduced 410 bills addressing student data privacy.
- 36 states have passed 71 student data privacy bills into law.

Legislative Landscape Prior to 2016

Following the 2014 legislative session, which focused primarily on the education data collected by states and districts, in 2015 states introduced legislation to **govern the data use and privacy activities of online service providers.** Last year states also introduced several bills that would **address the capacity and resource needs of districts, especially given the increased data privacy and security responsibilities many districts and school boards were charged with in 2014.** Several states introduced legislation describing a role for the state in supporting districts' privacy activities. These state roles included helping districts create and implement data privacy policies and provide staff training. In 2015 federal policymakers also became increasingly engaged in the student data privacy conversation. Several new federal bills focused on student data privacy, including measures proposing changes to the Family Educational Rights and Privacy Act and efforts to regulate service providers. Congress approved new privacy provisions as part of the latest version of the Elementary and Secondary Education Act, listing data use and privacy capacity building as allowable uses of the law's professional development funds.

2016 Summary

- 34 states introduced 112 bills addressing student data privacy.
- 14 states passed 16 new student data privacy laws.

In 2016 bills addressed many of the same themes as years past, though some states considered creative approaches to these themes. States introduced bills to take the following actions:

- Govern the data use and privacy activities of online school service providers.
  - Nearly half of the bills introduced (52) governed the data activities of online service providers.
  - Thirty-six bills (one-third of all bills considered this session) contained provisions modeled off of SOPIPA.
  - Forty-two bills included requirements for contracts between service providers and states or districts.
- Establish greater transparency around how states and districts are managing student information.
  - Sixty-nine bills contained transparency provisions, in many cases directed specifically at giving parents greater insight into the data that is collected on their children.
- Grant new responsibilities for safeguarding data to districts.
  - Forty-four bills proposed assigning new responsibilities to local education agencies. The type and scope of responsibilities varied, but most entailed establishing governance, increasing transparency, or placing new requirements on third-party contracting practices.
  - Eighteen bills contained a provision that addressed training or educators' capacity to use data; one passed into law.

This year, the share of bills that took a governance approach ticked up, and states considered a broader set of issues than in years past. Moving forward, states will likely continue to build on existing laws and may shift their focus to the role of privacy in the greater picture of how data is used to support student learning.

DQC
DATA QUALITY CAMPAIGN

2016 Session Overview

In 2016, for the third consecutive year, student data privacy was a priority issue for state legislatures across the country. While safeguarding students' personal information has always been an important concern, in 2014 this subject surged to the forefront of state (and federal) education policy conversations, driven in large part by the need to ensure that policies and practices account for new ways data is collected, used, and shared in the digital age and growing public concern about the lack of transparency around how school systems manage and use this information. This policy debate is not unique to education; technology has created capabilities to generate, analyze, and share data in unprecedented ways in every sector. This new landscape, coupled with a series of high-profile security breaches that have affected millions of Americans, has spurred a public appetite for greater accountability, restrictions, and transparency about information sharing practices writ large.

This year states were focused on the same core issues as in 2015, chief among them governance (or processes for making decisions about data use), transparency about states' data practices, and the activities of third-party providers that have access to student information. States, however, considered new creative approaches to these familiar themes this year.

The main questions states worked to address in 2015 were the same in 2016:

- How can schools use education technology, applications, and websites in support of student learning while still safeguarding student privacy?
- How can states best address the differences in the users and uses of data collected by the district and data collected through online services?
- How can states best implement privacy laws and support their districts' privacy policies and activities?
- How can states best develop privacy and data use policies that address immediate questions and concerns and allow for responsive governance decisions in the future?

Several new questions also rose to the forefront this year, such as the following:

- How do states ensure transparency for parents?
- What is the proper role of parental consent when it comes to collecting nonacademic data via surveys?
- How do we safeguard student privacy when the learning platform spans both school and personal life (e.g., take-home devices, social media)?

How Are States Protecting Privacy? Two Legislative Strategies

No matter which of these complicated issues a bill seeks to address, as in years past, student data privacy bills adopted two main approaches: protecting privacy by limiting data use (a "prohibitive" approach) and protecting privacy by implementing data governance (a "governance" approach). These approaches are not, however, mutually exclusive and often appear within a single bill.

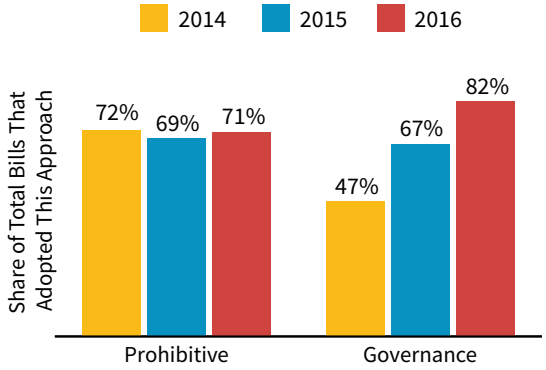
Prohibitive approach

- This approach seeks to ensure student privacy by preventing or halting the collection of a certain type of data (e.g., biometric data) or a certain data use (e.g., predictive analytics).
- The Data Quality Campaign's (DQC) analysis shows that 80 of 112 bills were introduced using this approach (about the same share as 2015).

Governance approach

- This approach seeks to amend or establish the procedures (e.g., security audits, public lists of data collected), roles and responsibilities (e.g., establishment of a chief privacy officer, description of school board and legislature roles), and supports (state leadership) needed to ensure that data is used appropriately.
- DQC's analysis shows that 92 of 112 bills—or 82 percent—were introduced using this approach (compared to 67 percent of bills in 2015).

LEGISLATIVE APPROACHES IN STATE STUDENT DATA PRIVACY LEGISLATION OVER TIME



The share of prohibitive bills has remained largely the same over the past three years, while the share of bills that addressed data governance has grown. Note that some bills contain both approaches.

Summary of Introduced Legislation

Between the start of each state's 2016 session through September 1, 2016:

- Thirty-four states considered 112 bills explicitly addressing student data privacy.
- Twenty of the 34 states considered numerous bills.
- States often considered bills articulating different approaches (i.e., governance and prohibitive or bills governing state data activities and the activities of third-party service providers).[1]

The student data privacy bills considered this session highlighted several key themes of importance to states.

Third-party service providers

The primary issue dominating privacy legislation in 2016 concerned the data shared between public education institutions and third-party service providers. Determining the role of policy in governing this relationship has been the subject of much conversation in states, given that using multiple private online providers to play a big role in learning, not just operations, is a relatively new practice for schools.

California was the first state to pass legislation that directly governs the activities of these service providers. Signed in September 2014, the Student Online Personal Information Protection Act (SOPIPA) places restrictions on the providers of online services and applications that are primarily designed for use in K–12 schools and have access to student personal information. These providers are prohibited from engaging in targeted advertising, amassing a profile of a student, or selling or disclosing student information according to specifications spelled out in the act, among other requirements. Because it was the first of its kind and garnered support from both the education sector and private industry representatives, SOPIPA has since become a model for other states considering legislation on this issue.

- Fifty-two bills were introduced that governed the data activities of online service providers, 36 of which contained provisions modeled off of SOPIPA or the SUPER Act, a similar model bill that seeks to govern online service providers. Though all of these SOPIPA-inspired bills contained at least some language identical to the original, they were not carbon copies. States built on California's model and in some cases adapted it for their own contexts.
    - For example, 23 of the bills modeled off of SOPIPA included a definition of targeted advertising, something not included in the original. Most of these definitions are similar or identical to the language that was included in federal legislation introduced in 2015 by US Representatives Jared Polis (D-CO) and Luke Messer (R-IN). Given the broad coalition of national education organizations, including DQC, that supported this legislation, the field clearly interpreted this language as a best practice. This targeted advertising definition is now law in Colorado, Connecticut, Hawaii, North Carolina, Tennessee, and Virginia.
    - California considered a bill that would apply SOPIPA's provisions to operators that were designed and marketed for preschool and prekindergarten purposes and have actual knowledge that their service is used for that purpose.
- Forty-two bills included requirements for contracts between service providers and states or districts. Some of these bills broadly required contracts to include provisions that safeguard privacy and security, while others indicated specific terms that must be contained in a contract, such as prohibiting a private vendor from selling student data.

Local role in safeguarding data

While much of the privacy conversation initially focused on student data that states collect, there has been increasing recognition of the important local role in safeguarding data.

FEDERAL PRIVACY LANDSCAPE

Unlike in 2015 when federal policymakers sought to address student data privacy through both new and existing laws, federal activity in 2016 focused on implementing the recently reauthorized No Child Left Behind (NCLB), known as the Every Student Succeeds Act (ESSA). Likely presaging a focus of state legislation in 2017, ESSA rulemaking this year required the US Department of Education and state education agencies to consider broad questions about education data use and reporting for both accountability and transparency purposes. ESSA maintains NCLB's strong focus on data and requires states to redesign their accountability systems; produce new postsecondary, attendance, and financial indicators; report on more groups of students, including those who are homeless or connected to the military; and engage stakeholders to design new public reports that will make data useful to the public. For the first time, data privacy and literacy training are listed as allowable uses of the law's Title II funds.

While student data privacy is likely to be a subject of renewed federal interest next year, federal policymakers may carry forward the more contextualized view of data they adopted this year to think carefully about how they can best support and strengthen state data practices and privacy protections.

1 See the Bill Index at the end of this paper for more details on the types of bills introduced and signed into law.

- Forty-four bills proposed new responsibilities for local education agencies (LEAs). The type and scope of responsibilities varied, but most entailed establishing governance, increasing transparency, or placing new requirements on third-party contracting practices.

- Eighteen bills contained a provision that addressed training or educators' capacity to use data; one passed into law.

    - Minnesota introduced a bill that would require districts to conduct annual trainings for at least one staff member with access to student data to ensure compliance with the Family Educational Rights and Privacy Act.

While some states thought about how they could support local school systems in their capacity to safeguard data, especially given the new responsibilities prescribed in state laws, there is still a long way to go. Some bills did address training, but many were geared toward security and technology staff, rather than classroom teachers. Given the importance of ensuring that those closest to students are trained on how to protect and use students' personal information ethically, responsibly, and in accordance with new state laws, state legislatures should prioritize this issue more in the future and consider the role of teachers in addition to technology staff—especially (but not only) in cases in which new state student data privacy laws have implications for classroom data use. See DQC's brief on educator data literacy for more recommendations on how state policy can support educator data use.

BEYOND SCHOOL DATA: NEXT GENERATION OF STUDENT PRIVACY CONCERNS

More than ever before, schools are using new devices and digital platforms, such as online games and social media, to create new learning opportunities for students inside and outside the classroom. These innovations can blur the lines of a student's school and home life and introduce new questions about how to establish privacy protections for youth that are more connected than ever before. This session, several states considered legislation to address such questions. Four states introduced seven bills to govern the management of students' personal information stored on devices that are part of school 1:1 device programs. The American Civil Liberties Union put forth omnibus model legislation to address student information system privacy, 1:1 device programs, social media, and other surveillance issues. While many of these and similar bills venture outside the scope of traditional student data privacy issues, they represent a significant evolution and broadening of the student privacy and educational technology conversations and highlight a growing appetite to address the privacy implications of our increasingly connected schools.

Transparency for parents

Transparency about data practices and privacy policies is just as important as updating them. The public, and parents in particular, are hungry for more information about why student data is collected, how it is used and protected, and who has access to it.

- Sixty-nine bills sought to establish greater transparency around how states and districts are managing student information. In some cases, these transparency provisions provided for publishing a "data inventory," or list of all of the elements that a state or district collects. Some bills went further and called for an explanation of why that data is collected, which helps provide more context for parents and the public as to the value and purpose of this collection.

- Several states considered bills containing provisions focused on transparency for parents. These bills took many forms, but in many cases they manifested new proposed responsibilities for LEAs and targeted specific instances in which parents should have access to data, rather than a more systematic or governance approach.

    - Tennessee considered two identical bills that would require an LEA to notify a student's parents by automated email each time the student's educational record or personal information is accessed and to maintain a record of when, why, and by whom student education records or personally identifiable information is accessed.

    - Rhode Island considered a bill that would require parents to have access to a student's state assessment booklet and answer sheet after results are released.

    - Georgia considered a bill that would require an LEA to give students and parents a formal written explanation of the goals and capabilities of any digital learning platform. It would also require LEAs to use only digital learning platforms that include a parent portal allowing access to the platform and all of the content available to the student.

While well intentioned, these narrowly focused bills give parents the opportunity to monitor a particular instance of data collection, without giving them a more comprehensive picture of actionable data they can use to partner in their child's education. While there is broad agreement in states that transparency is important, there are no concrete, universal guidelines for what meaningful transparency looks like when it comes to student data privacy and the role of legislation in promoting and supporting that transparency. Parents deserve access to information, but it is important to be thoughtful about what questions they have and what they most need to know.

SURVEYS AND THE COLLECTION OF NONACADEMIC DATA

More than a dozen states introduced bills this session that would limit the use of nonacademic student surveys, primarily by requiring parental notification and consent (in other words, "opt-in") for the administration of such surveys.

Most of these bills drew language from the Protection of Pupil Rights Amendment (PPRA), which is a federal law that requires schools to obtain parental consent prior to administering certain types of surveys on enumerated nonacademic topics such as sexual behavior, political affiliation, and criminal behavior. These bills would apply similar restrictions to surveys administered on behalf of the state or districts.

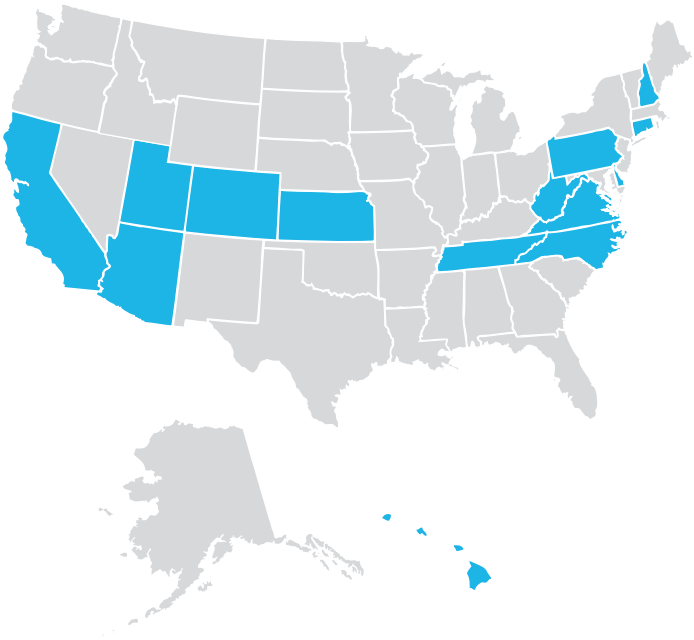
Arizona passed a law that requires parental consent prior to the administration of student surveys on the topics enumerated in PPRA and requires the state Board of Education to approve in a public meeting any student-level nonacademic data before it is included in the statewide longitudinal data system.

New Hampshire Governor Maggie Hassan vetoed a similar bill that would have required parental consent for nonacademic surveys. The state already has a law in place that requires parental notification and the ability to opt out of these surveys. The governor argued that such a bill "would present an undue burden to schools administering a survey and undoubtedly lead to unreliable survey data, creating insurmountable barriers to conducting meaningful school-based research used to promote the well-being of New Hampshire children, families, and communities."

While most of these bills focus on the survey instrument, the intent appears to be to place guardrails (in particular a greater role for parents) and more transparency around the collection of nonacademic data—often measured via surveys. This issue is not going away and will be increasingly complex given that states are now required to incorporate a nonacademic indicator in their accountability systems under the Every Student Succeeds Act and states are looking at surveys as a potential measurement instrument. As a result, states will have to be more intentional and transparent about the purpose of the nonacademic data they collect.

Summary of New State Laws

As of September 1, 2016, 16 student data privacy bills had been signed into law in 14 states. These states represent differing political and regional environments. Eleven of these states had already passed privacy laws in the past two years. This session Arizona, Hawaii, and Pennsylvania passed their first student data privacy laws.



Fewer new laws were enacted this year than in 2015 and 2014. These new laws address a diverse set of issues, the most prevalent of which are governing the activities of service providers and increasing transparency.

Governing the activities of third-party service providers

- Seven states passed seven laws this session containing provisions that were directly modeled off of SOPIPA and prohibit service providers from engaging in targeted advertising, amassing a profile on a student, and selling student data, among other restrictions.
    - Since 2014, 33 states have considered a bill and 17 states have passed a law modeled off of SOPIPA. States will continue to iterate, but clearly SOPIPA has become the standard.
- Five new laws contain new contracting requirements.
- Colorado and Connecticut passed bills into law that distinguish between those third parties with which schools have a negotiated contract and those that do not have a formal contract. This is the first time this strategy has appeared in student data privacy legislation. States may seek to replicate this approach next year.

COLORADO ENACTS FAR-REACHING BIPARTISAN PRIVACY LAW

In June 2016, Colorado Governor John Hickenlooper signed a bipartisan student data privacy bill into law that places new restrictions on the activities of school service providers, charges districts to be more transparent about how data is used and shared, and requires the state to support districts' capacity to safeguard data. The Student Data Transparency and Security Act, which builds on Colorado's 2014 student privacy law, prescribes broader and more stringent responsibilities for the state, districts, and service providers than most other laws over the past three legislative sessions. Some key provisions worth noting include the following:

- **Distinguishing types of service providers.** Like many other state bills this legislative session, the law issues requirements for school service providers that are largely modeled off of California's 2014 SOPIPA, including that individual student data may not be sold or used for targeted advertising. But the law goes beyond SOPIPA to distinguish between providers with formal contracts and those that are used by teachers or other school staff without formal negotiated contracts. While both formally negotiated contracts and "click wrap" agreements are considered legally binding, the latter undergo a different level of scrutiny and review. In making this distinction, the law recognizes this difference in the circumstances surrounding how schools engage with these services.
- **Increasing transparency around data use and sharing practices.** Each district and charter school is required to publish on its website a list of the data elements that it collects and maintains and how they are used; each of the services it formally contracts with; and "to the extent practicable," each of the on-demand providers that are used by its employees. While transparency can help safeguard privacy and build public trust in data, some are concerned that these new requirements will place a heavy administrative burden on districts.
- **Providing state support for local capacity.** This law is unique in its explicit focus on training local staff to use student data, an issue most other state student data privacy bills have largely left unaddressed. The Colorado Department of Education must identify and make available to local districts resources that they may use to train employees on student information security and privacy. Developing these trainings and resources for districts will likely be a significant project for the state but one that is critical to ensuring that those working closest to students have the knowledge and supports to use data effectively and ethically.
- **Requiring districts and charter schools to adopt a privacy policy.** The law requires districts and charter schools to develop a student information privacy and protection policy that adheres to the provisions of the law. Acknowledging that not all districts have the capacity and expertise to craft a comprehensive policy of their own, the Colorado Department of Education must draft a model policy that districts can adopt.

The law went into effect in August 2016. Especially given that the provisions above are largely unique compared to other state laws, and will require a significant effort on the part of the state and districts, it will be important to watch and learn from Colorado's implementation of this law as it may become a model for other states.

Governance and transparency for state data practices

- Five new laws provide for new state-level governance and transparency practices.
  - Utah's law tasks the state board with developing a student data privacy governance plan, establishing advisory groups, and designating a state student data officer.
  - Arizona's new law requires the state board to approve all nontest data (or data not relating to a core subject) that is included in the statewide longitudinal data system and post the list of these indicators, along with the reason for collecting them and with whom the data is shared, on the state's website.

New roles for LEAs

- New state laws in Arizona, Colorado, Connecticut, and Utah assigned new responsibilities to LEAs.
  - Utah requires all LEAs to develop their own data governance policies and establish a student data privacy manager. The law also requires the state to establish a data users advisory group composed of individuals who use student data in districts and schools, which will provide feedback on the practicality of proposed state data use policies. The state student data privacy officer is required to provide training, support, and model governance plans to LEA employees.

- Connecticut requires local or regional boards of education to notify parents within five business days each time a new contract is signed that would affect their child. This electronic notice must include a brief description of the purpose of the contract and what student information may be collected as a result.
- Both Utah's and Colorado's (see sidebar on p. 6) laws require some state support for these new local responsibilities. Connecticut's law establishes a task force to study issues relating to student data privacy, including the feasibility of developing a toolkit for use by local and regional boards of education to support practices critical to safeguarding data, such as contracting and security.

Updates to legislation

- Five of the 16 new laws were relatively small amendments to laws that were passed since 2014.
  - Virginia made amendments (HB 519 and HB 749) to a 2015 law governing the activities of service providers. These amendments include additional definitions, which largely make the law more in line with legislative approaches that other states and the federal government are considering. The law will also now cover services designed and marketed for schools that are used by a "school-affiliated entity," or a private entity that supports schools (e.g., booster clubs or PTAs).

Student Data Privacy Legislation over Time

To date, **49 states and the District of Columbia (all but Vermont) have introduced at least one student data privacy bill, and 36 states have at least one new student privacy law.**

Over time, bills have become more focused on data governance, and fewer bills would compromise the basic functioning of the state's education services.

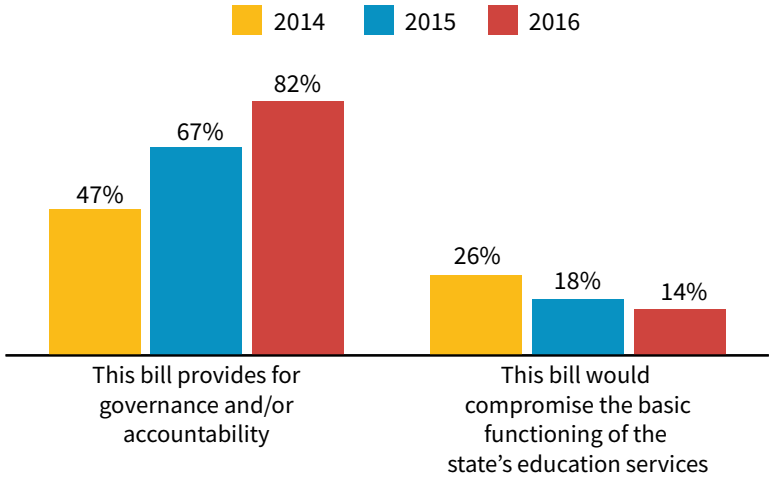
- In 2014 a quarter of the bills introduced would compromise the basic functioning of the state's education services, compared to 2016 when that proportion was 14 percent.
- In 2014 less than half of the bills provided for governance; in 2016 82 percent of them did.

States are also building on their past efforts.

- Twenty-one states that had already passed a law in 2014 or 2015 introduced bills this session.
- Ten states introduced a bill in 2016 that would amend a law passed in 2014 or 2015.

The work of safeguarding privacy is never done, and it is encouraging to see states go back and build on the work they have already done. These bills also are considering more diverse issues, signaling that states are adapting for their own contexts and thinking more broadly about data and privacy in schools. In contrast to 2014, now there are more resources and models to inform this work.

TRENDS IN STATE DATA PRIVACY LEGISLATION 2014–16



Looking Ahead to 2017

Next year DQC anticipates the landscape of student data privacy legislation will continue to evolve, as states build on the conversations that have already been started in nearly every statehouse while they work in a new policy environment created by the federal Every Student Succeeds Act (ESSA). There is broad acknowledgment across the country about the need to prioritize and address student data privacy and a growing appetite to establish data governance as a policy solution. DQC hopes that these new contexts will drive states to think more broadly about how data is used in service of student learning and start to think about privacy as just one piece of the full picture of data use. DQC has released a new set of state policy recommendations and will be making adjustments to our legislative tracking and reporting in accordance with changes in the field and what we hope to see states work on moving forward.

What to expect next session

States will:

- **Address the role of third-party service providers.** This issue will likely remain an important point of contention for states, especially in the absence of movement on this issue in Congress. In 2016 states introduced several innovative approaches to legislating this issue, such as the approach used by Colorado and Connecticut to distinguish between providers with and without contracts—and next year other states may follow suit.
- **Amend existing privacy laws and focus on their unique state contexts.** Like this year, states likely will make small amendments and continue to refine existing student data privacy laws based on their individual state needs and continued conversations about how best to safeguard data.
- **Explore student privacy issues beyond the education record.** Given that these issues are still very new, next year there will likely be even more conversation about the privacy implications of new technology-driven school practices that span a student's school and home life.
- **Turn attention to ESSA, and the number of bills narrowly focused on privacy will decrease.** Moving forward, the number of bills and new laws focused specifically on student data privacy will likely continue to decrease. States will be most focused on their new responsibilities under ESSA, in particular their need to develop accountability plans in accordance with the law. These plans will require states to think about indicators and understand the needs of their data systems.

What should states do?

- **Approach new privacy protections in the broader context of how data serves student learning.** Privacy is and will continue to be critical, but it is just one piece of this picture. DQC encourages states to shift from narrow prohibitions on individual uses of data to provisions that establish governance. Strategies for governing data management and use should be driven by the full picture of how data best serves student learning. This picture includes considering the other institutions and programs that serve students beyond the classroom and beyond K–12. ESSA contains numerous opportunities for states to go above and beyond to ensure that data works for educators, students, and families, and DQC hopes that the attention on ESSA implementation will lead states to focus on the broader picture of data use—and the important role of privacy policies within that picture.
- **Prioritize, promote, and support local capacity.** Everyone has a role to play in safeguarding data, but states have largely ignored the important need to ensure that all people who interact with student data have the ability to safeguard it and use it to advance student learning. Despite growing consensus and awareness of the importance of training, very few bills this year contained provisions that would support the ability of those closest to students, and in particular classroom teachers, to understand their role in safeguarding students' personal information. Moving forward, states should consider the role of legislation in supporting educators' ability to safeguard data, especially as they propose new responsibilities for data use in districts and schools.
- **Learn from and address implementation challenges.** As states borrow from each other and revisit and amend their own laws, it is important to remember that many of these laws have only recently gone into effect; there is still a lot to learn about how they play out in practice. SOPIPA, a model for many state bills and new laws, went into effect only in January of this year. Given the number of new laws that have been enacted in the past three years, and given that in many ways these policy solutions are new and untested, DQC hopes that states will find ways to track implementation of new laws and identify and address unanticipated consequences and challenges.

Time to act: New DQC recommendations and future research

In April 2016, DQC released a new set of policy recommendations that provide a guide for states to ensure that data is working in service of student learning. The Four Policy Priorities to Make Data Work for Students are the following:

1. Measure what matters. Be clear about what students must achieve and have the data to ensure that all students are on track to succeed.
2. Make data work for students. Provide teachers and leaders the flexibility, training, and support they need to answer their questions and take action.
3. Be transparent and earn trust. Ensure that every community understands how its schools and students are doing, why data is valuable, and how it is protected and used.
4. Guarantee access and protect privacy. Provide teachers and parents timely information on their students and make sure it is kept safe.

DQC will be evaluating states' progress toward each of these priorities, and we will be considering legislation as part of this evaluation. Given what we anticipate will be a shift in states' activities we will be broadening our legislative tracking to all state bills that affect data use. We will also begin to research, analyze, and share how states are implementing laws they pass that have a major impact on data use practices in their states.

We hope states will continue to prioritize privacy as a critical piece of making data work for students.

2016 Privacy Legislation Index*

What the bill addressed	Number of bills	Number signed into law
PROHIBITIVE VS. GOVERNANCE/GOVERNANCE FOR USE OF STUDENT DATA		
Prohibitive approach	80	12
Governance or accountability approach	92	12
Both approaches	67	11
SCHOOL BOARD ROLES IN LEGISLATION		
Gave state boards privacy-related responsibilities	13	4
Gave district or county school boards privacy-related responsibilities	10	3
ROLE OF SERVICE PROVIDERS (THROUGH DIRECT GOVERNANCE OR CONTRACT REQUIREMENTS)		
Addressed data activities of vendors	52	9
Required criteria or guidelines for contracts with service providers	42	5
ROLE OF LEAs		
Described privacy or security responsibilities for LEAs	44	4
DEFUNDING OF STATE LONGITUDINAL DATA SYSTEMS		
Sought to prevent the continued or expanded funding of the state longitudinal data system	8	0
OPT-OUT		
Allowed parental opt-out of data collection or the submission of personally identifiable information to third-party service providers or consortia	42	5
TRANSFER OF STUDENT DATA OUTSIDE THE STATE		
Prohibited the transfer of student data outside the state in at least some circumstances	16	0
DATA BREACH NOTIFICATION PROCEDURES FOR STUDENT DATA BREACHES		
Required implementation of a breach notification process	22	2
PROVISIONS OF OKLAHOMA HB 1989		
Adopted many of the provisions outlined in 2014's Oklahoma HB 1989	8	0
PROVISIONS OF CALIFORNIA'S 2014 SOPIPA LAW		
Adopted many of the provisions of California's 2014 SOPIPA law	36	7
TRANSPARENCY REQUIREMENTS		
Required increased transparency	69	12
STAFF TRAINING		
Provided for data privacy or security training	18	1

**Note: The District of Columbia is counted as a state for the purposes of this analysis.*

DQC
DATA QUALITY CAMPAIGN

The Data Quality Campaign is a nonprofit policy and advocacy organization leading the effort to bring every part of the education community together to empower educators, families, and policymakers with quality information to make decisions that ensure that students excel. For more information, go to www.dataqualitycampaign.org and follow us on Facebook and Twitter (@EdDataCampaign).