

Student Data Privacy Legislation

What Happened in 2015, and What Is Next?

EXECUTIVE SUMMARY

Last year, growing state and district use of education data and increased public attention to the ways in which these data are collected, used, managed, and disclosed sparked much conversation in statehouses around the country about the value of data and how they are protected. Student data (e.g., demographics, transcripts, attendance, test scores, outcomes, etc.) are an important tool for policymakers, educators, and families as they seek ways to support students and improve education experiences and pathways. Safeguarding data is a critical component of effective data use, and this complex and critical issue has continued to evolve over the last year. The student data privacy bills introduced in 2015 reflect both continued and newly developing student data privacy conversations in states and at the federal level.

IN 2014:

- 36 states introduced 110 bills addressing student data privacy.
- 21 states passed 24 new student data privacy laws.

In 2014, many state student privacy bills focused on the data collected by states and the perceived role of the federal government in collecting and accessing student data. While these issues have continued to be prominent, the latter half of the 2014 legislative session was marked by a shift in focus from the data in state systems to the data and privacy activities of third-party service providers. This conversation culminated in California's passage of an innovative new law, the Student Online Personal Information Protection Act (SOPIPA), which directly governs the activities of online service providers, rather than the state agencies or districts that may contract with them. Although the law does not go into effect until 2016, it has provided a model for many state and federal policymakers to adopt and adapt.

IN 2015:

- 46 states introduced 182 bills addressing student data privacy.
- 15 states passed 28 new student data privacy laws.

In 2015, states largely picked up where 2014 left off and began introducing legislation to do the following:

- Govern the data use and privacy activities of online service providers.
 - Twenty-five states introduced legislation modeled on California's 2014 SOPIPA law, although many states made alterations to fit their own needs and to reflect an evolution in thinking through many of the most complex and nuanced aspects of the original law.
 - Thirty-one states introduced legislation that articulated contract requirements for service providers.
- 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 last year.
 - 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.

During 2015, federal policymakers also increasingly engaged in the student data privacy conversation. Student data privacy was the focus of several new federal bills as well as the subject of a key amendment to the Senate's bill to reauthorize the Elementary and Secondary Education Act and a proposed amendment to the Family Educational Rights and Privacy Act.

By summarizing the activity of this legislative session with regard to student data privacy, stakeholders can better understand the continuing evolution of the student data privacy conversation and how legislation, coupled with policies, guidance and support, and clear and transparent communication, can best aid the use of education data in the service of learning while ensuring that students' privacy is safeguarded.

SUMMARY AND ANALYSIS

EVOLUTION OF THE PRIVACY CONVERSATION





Safeguarding privacy is a critical component of effective data use and, over the last two years, has emerged as a legislative priority in nearly every state. The topic moved into the spotlight in early 2013 owing to growing concerns about the appropriate use and risks of collecting education data, as well as privacy concerns related to data collection and use by organizations in almost every area of public life—from the National Security Agency to Target.

This growing national discourse about data provided an opportunity for conversations about the value of education data, but it also created a context in which many state policymakers and education leaders felt they needed to take action in response to either an immediate and specific situation (e.g., contracting with inBloom, implementing the Partnership for Assessment of Readiness for College and Careers or Smarter Balanced Assessment Consortium tests) or to more general concerns about government overreach, the implications of collecting information on individuals, and the activities of online data service providers.

In 2014, the privacy conversation in states focused heavily on questions about the student data activities of

state and federal governments. While these important conversations have continued, much of the national conversation has shifted to questions about the activities of service providers and how student data are accessed and shared among state agencies and entities.


While the privacy conversation is different in every state, many legislators in 2015 heard similar concerns and questions around common topics:

-  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 the use of 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?


The Federal Privacy Landscape

Unlike in 2014, student data privacy conversations in states in 2015 were influenced by parallel bipartisan conversations at the federal level, even as the states' approaches informed these federal conversations. This year federal lawmakers sought to address student data privacy through both new and existing laws.


Much of the data privacy conversation at the federal level in 2015 has centered on two existing federal laws:

-  Representatives Todd Rokita (R-IN) and Marcia Fudge (D-OH) introduced an amendment to the [Family Educational Rights and Privacy Act](#), the primary federal law regulating the [disclosure of student records](#). While the amendment will undergo additional revisions, the current bill clarifies some data use provisions and increases the federal


government's enforcement authority over service providers that misuse student data.

-  In its version of a bill to reauthorize the [Elementary and Secondary Education Act](#), the primary federal law addressing federal education funding, accountability, and reporting requirements, the Senate adopted [an amendment](#) introduced by Orrin Hatch (R-UT) and Edward Markey (D-MA) to create a Student Data Privacy Policy Committee to study and make recommendations on privacy safeguards and parental rights.

Federal policymakers also introduced legislation independent of existing federal statute:

-  Representatives Luke Messer (R-IN) and Jared Polis (D-CO) introduced the [Student Digital Privacy and Parental Rights Act](#), based on California's Student Online

Personal Information Protection Act, to regulate the activities of online service providers that collect student data through students' use of the service.

-  Senators Steve Daines (R-MT) and Richard Blumenthal (D-CT) introduced a similar bill, the [SAFE KIDS Act](#), in the Senate.

These efforts communicate federal policymakers' growing commitment to [their unique role in safeguarding student privacy](#). Ideally federal efforts will complement state efforts, rather than impede them; it is possible that the fact that states introduced more legislation in 2015 than in 2014 but did not pass significantly more laws suggests state hesitation in light of a shifting federal landscape. Federal policymakers must think carefully about how they can best support and strengthen state protections.


Advertising: The Good, the Bad, and the Ugly


One of the most important and nuanced privacy issues that state and federal lawmakers faced this year was legislating the use of student data by online service providers, apps, or websites to personalize learning by suggesting to students additional activities or experiences within the program. For example, a service could use a student's performance on a math quiz to recommend an appropriate learning activity on an aspect they struggled with.

While policymakers are understandably eager to ban the use of student data for commercial or marketing purposes, including "targeted advertising" (i.e., showing advertisements to students based

on the information they may provide about their interests and achievements), legislative language prohibiting the use of student data for these purposes can unintentionally limit the use of student data by a service provider to cultivate a personalized and adaptive learning experience for the student.

Despite the complexity of this issue, several state and federal bills have parsed out the difference between using data for advertising and using the student's performance and activities within the service to make recommendations for additional learning activities.


 One way to ensure that services can personalize the student experience is to include an allowance for service providers to use data from a student's current visit to the site or service to guide the student's experience within the program, while still prohibiting the creation of a student profile or the storage of data over time.


 States are also building in provisions for "recommendation engines" that direct a student's activities within a program based on his or her activities in that same program.

Provisions like these help ensure that student data are not used for commercial purposes but can be used to harness the potential of technology and online services.


Regardless of how states attempted to answer these questions through legislation, their 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).

 Data Quality Campaign's (DQC) analysis shows 125 of 182 bills were introduced using this approach (compared to 79 of 110 bills in 2014).




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 (e.g., state leadership) needed to ensure that data are used appropriately.

 DQC's analysis shows 122 of 182 bills were introduced using this approach (compared to 52 of 110 bills in 2014).

SUMMARY OF INTRODUCED STATE LEGISLATION


From the start of each state's 2015 session through August 24, 2015:

-  Forty-six states considered 182 bills explicitly addressing student data privacy.
-  Most (38) of the 46 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.

THE ACTIVITIES OF ONLINE SERVICE PROVIDERS

States sought to introduce bills that articulate ways online service providers can use student data in the service of learning while also instituting prohibitions on using data for commercial purposes.

 Twenty-five states introduced legislation modeled on California's 2014 Student Online Personal Information Protection Act (SOPIPA) law, although most states made alterations to fit their own needs and to reflect continuous developments in the field's thinking about how to best structure and operationalize these types of protections. Adjustments made by states included expanding the scope to include higher education

¹ See the 2015 Privacy Legislation Index at the end of this paper for more details on the types of bills introduced and signed into law.

Opt-Out: Is It about Privacy?



In 2014, 17 student data privacy bills introduced in states included provisions to allow some type of opt-in or opt-out for the collection, use, or disclosure of student data. Thirteen of these bills would have allowed parents to opt out of data collection, the disclosure of directory information (which is already provided for under federal law), or the submission of personally identifiable information to third-party service providers or consortia. In 2015, the number of student privacy bills with opt-out or opt-in provisions grew to 78, with states introducing bills to allow parents to opt out of activities including district or state data collections, research studies, and data sharing outside the district.

While opt-out may be a parental right in some cases, it is not necessarily a privacy protection

and should not be treated as such in legislation. Privacy experts from the Future of Privacy Forum (FPF) **note that** “providing parents with more notice and choice may do little to actually protect student privacy.” In many cases opt-out serves only to shift the burden of risk assessment to the parent without the context to make an informed decision or actually providing any additional privacy protections.


There can be appropriate uses for opt-out, such as for data uses not related to educational services; the Family Educational Rights and Privacy Act, for example, allows parents to opt out of having their child’s directory information (which can include name, address, photo, school enrollment, etc.) shared. However, rather than using opt-out as a way to protect data,

most state and federal legislation on opt-out seem to highlight two main concerns:

-  a perception that the state or federal government is intruding into education content or assessment decisions
-  concerns about the relevance or politics of the assessment consortia associated with the Common Core State Standards

FPF notes that rather than relying on opt-out provisions “to foster an environment of trust, schools and their education partners must offer more insight into how data is being used.” While debates about opt-out are certain to continue, it is critical that the issues of opt-out and the value of education data and use are not conflated with student data privacy protections.

or early childhood programs in addition to K-12 and permitting the use of “recommendation engines” (see “Advertising: The Good, the Bad, and the Ugly” on page 3).


-  Thirty-one states introduced bills articulating contract requirements for service providers. Common requirements included having privacy and security policies in place and stating that they would not sell student data or use them for secondary purposes.

The increasing use of technology in the classroom is setting the stage for incredible new uses of data to support students and personalize their education experience. States that create clear yet adjustable laws (like those based on SOPIPA or those that describe contracting requirements) and governance bodies to determine the permissible activities of online providers will be prepared to address current privacy concerns and make thoughtful, informed decisions in the future. It is also critical that states continue to investigate the ways technology and data can be used in the service of learning and ensure that state laws and policies do not unintentionally prohibit these helpful practices.

SPECIFYING WHY AND UNDER WHAT CIRCUMSTANCES RESEARCHERS CAN ACCESS DATA

Along with online service providers, researchers and their permissible access to data were a focus of state legislation this year, with some states articulating

governance and data request review processes and other states seeking to limit researchers’ access to data.

-  Sixty-one bills explicitly addressed research activities or researcher access to student data.
 - Six of these bills were signed into law in five states.
 - Of those bills signed into law, five describe the legitimate research purposes for which data disclosures may be appropriate.
 - The other new law, passed in Arkansas, limits state data disclosures, including to researchers without parental consent, and does not describe additional data governance measures.

Research plays a unique and integral role in education by helping to identify best practices, apply resources responsibly, and prepare all students for success. Without research, states would lack the analysis and contextualized information they need to make informed decisions on everything from curriculum and programming decisions to teacher and school effectiveness. States have a responsibility to implement strong data governance processes, create detailed research request review and approval policies, and develop a state research agenda to harness the capacity of researchers to meet the state’s needs. The five new laws that describe legitimate research purposes help ensure that researchers have appropriate access to student data while student privacy is safeguarded.

LIMITING DATA SHARING WITHIN OR ACROSS STATE LINES OR BANNING DATA INITIATIVES OUTSIDE OF K-12

A significant number of introduced bills (20) sought to prohibit or severely limit the transfer of at least some data outside of the state.

- No new state passed a law with these provisions in 2015.
- Louisiana enacted these prohibitions in a student data privacy law passed in 2014. While the original law was amended this year, in part to address some of the law’s unintended consequences, this provision was not altered.

Some bills (11) would have prevented most instances of linking or sharing data across state agencies or sectors, either through express prohibitions or through requirements so burdensome as to be prohibitive.

- No new state passed a law with these provisions in 2015.
- Louisiana enacted these prohibitions in a student data privacy law passed in 2014. While the original law was amended this year, in part to address some of the law’s unintended consequences, this provision was not altered.

Thirteen bills sought to prohibit the use of data for economic planning or workforce development. Many of these bills employed the same language, suggesting this provision has a single origin and was shared across states.

- None of these bills were signed into law.

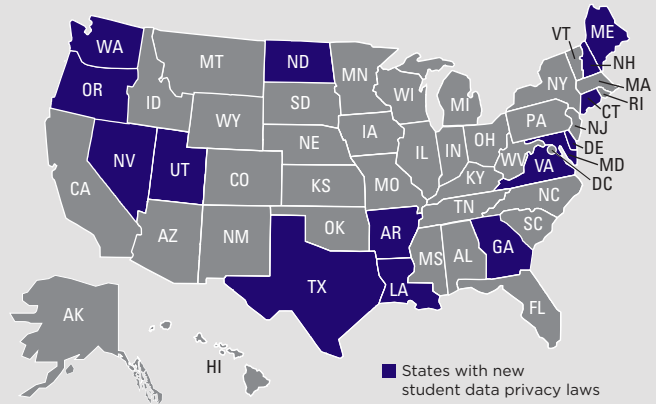
Twenty-three bills prohibited or severely restricted states’ ability to collect social and emotional learning data, including student surveys requiring parental consent.

- None of these bills were signed into law.

Without limited and secure linkages between state agencies and across state lines, states are unable to understand how their schools are preparing students for success at college and in their careers, provide teachers or parents with a complete picture of their student, or answer the state’s own critical questions about policy and best practices across the P-20/workforce pipeline. States that prohibit or drastically limit these secure and limited linkages risk losing the ability to carry out these critical activities. Louisiana passed a law in 2014 to limit data sharing within the state. Already the state is facing widespread and disruptive consequences and is having to develop complicated workarounds.

SUMMARY OF NEW STATE LAWS

As of August 24, 2015, 28 student data privacy bills have been signed into law in 15 states. These 15 states represent a diverse cross-section of the country. The states represent different regions and political environments.



THE NEW PRIVACY LANDSCAPE

These 28 new state laws have created a new data privacy landscape in states across the country.²

ROLE OF SERVICE PROVIDERS AND CONTRACTS


Whether through laws that directly govern service providers or through contracting requirements, 13 new laws address the role of service providers in safeguarding student data.

Ten new laws are modeled at least in part on California’s 2014 SOPIPA law to explicitly govern the permissible activities of online service providers.

- Most states that introduced bills based on the SOPIPA model adapted it to meet their own needs. Examples include the following:



² For more information on each of the new laws, see www.ferpasherpa.org.

- » **Illinois** adapted the language to also apply to providers serving higher education institutions.
- » **Maryland** passed a law that expanded the coverage to include prekindergarten settings in addition to altering the definition of online service provider to refer only to those with contracts with public schools or districts.
- » **Georgia** passed a law that embedded the language into a larger student data governance and privacy law.

 Ten new state laws require specific contracting practices or provisions for service providers who collect and/or have access to student data.


DISTRICT, STATE BOARD, AND SCHOOL BOARD ROLES


Like last year, state legislation this year frequently charged districts, state boards of education, and occasionally local school boards with enacting, enforcing, or investigating student data privacy policies and practices.


-  Sixty-three introduced bills (nine of which were signed into law) gave school districts additional privacy- or transparency-related responsibilities.
-  Thirty-five introduced bills (five of which were signed into law) gave state boards privacy-related responsibilities.

WHAT SHOULD STATES DO NOW?

The 2015 legislative session is leaving states, districts, and service providers with new roles, responsibilities, opportunities, and challenges. As states continue to legislate around student data privacy and begin to implement and operationalize their laws, what should they be considering to help ensure that they are safeguarding privacy and supporting the state's use of education data in service of learning? DQC recommends that states take the following actions:




 **Provide transparency.** While the student data privacy conversation has evolved significantly from its often fear-inspired origins, misconceptions and opacity continue to fuel concerns and potentially damaging legislation. By being transparent about what data they collect, how and why the data are used, who has access to the data, and how the data are safeguarded, states can help curb concerns about

 Twenty-three introduced bills (seven of which were signed into law) gave local school boards privacy-related responsibilities.



 Some of the most common local responsibilities were rule-making, implementing and monitoring privacy and security policies, managing record requests, and creating and maintaining publicly accessible online data directories.

STATE SUPPORTS FOR DISTRICTS

In 2014, 28 state bills and 9 new state laws identified the school district as an important actor by charging the district with responsibilities in safeguarding student data privacy and ensuring data quality. This year, as some states continued to expand local roles, other states picked up this thread and began to consider how the state could best support districts in meeting these new responsibilities. Examples include the following:

-  **North Dakota** passed a law implementing data governance, transparency, and supports including data use training for any employee with access to student data.
-  **Virginia** passed a law to direct the state to develop a model data security plan for districts and to designate a chief data security officer to assist local school divisions with the development or implementation of data use and security policies.
-  **Nevada** passed a law that instructs the state to develop a security policy for districts to follow.

data use and privacy and communicate more effectively with the public.


-  **Communicate the value of data.** By using data to provide valuable information, tools, and services to educators and families, states can help take privacy conversations out of a vacuum and contextualize the use of data as a tool to support students. When educators and families get real benefits from education data—such as clear public reports, including school report cards and high school feedback reports, and parent and teacher data dashboards—they can truly see the value of education data and advocate for their use.
-  **Support boards and districts.** Districts, state boards, and school boards are uniquely positioned to understand local conditions and meet local needs. Many states are now calling on districts, state boards,


and school boards to take on new responsibilities related to data privacy and management. However, they cannot adequately meet these new responsibilities without additional supports from the state. As discussed above, some states are already


beginning to provide training, model policies, and direct support to districts. However, with a rapidly changing field and limited supports from the federal government (especially around data training), districts and boards will continue to need state support.

WHAT TO EXPECT IN 2016

As the 2015 legislative session concludes in most states, the themes, approaches, and evolving privacy conversations across the country suggest numerous implications for next year's state legislative sessions.³ Strategies states are likely to adopt in the future include the following:

-  Introduce bills that support the innovative, effective, and protected use of data. The recent conversations about student data privacy have naturally fed into conversations about why educators, families, districts, and states use education data in the first place. This year, states introduced a host of bills to ensure that student data are used in ways that improve educational experiences for students and provide more transparent and useful information to those who need it. From [Minnesota's](#) bill to create [student data backpacks](#) and empower parents to [Florida's](#) bill on [early warning systems](#) that help keep students on track for success, bills like these ensure that data are used to support students as they are safeguarded.
- As an outcome of shifting the privacy conversation—from one entirely focused on privacy to the ways data can be used effectively and responsibly—combined with increasing federal action and potential regulation or guidance, DQC believes that states may introduce fewer student data privacy bills in 2016.

 Convene education and privacy leaders along with educators and parents to discuss education data privacy topics. This year several states introduced a bill to create a committee or task force to study and make recommendations on student data privacy issues (an approach also adopted in the Senate's Elementary and Secondary Education Act bill, see "The Federal Privacy Landscape" on page 2). Additional states may choose to consider this approach, as it allows states to consult diverse stakeholders and experts and develop a coherent approach to privacy and data use that addresses immediate questions and creates a structure to investigate emerging issues and make decisions.

 Increase focus on other aspects of privacy in education, such as teacher privacy and the privacy of health records. This year, 13 of the student data privacy bills states introduced also addressed teacher privacy. In addition, questions about how students' medical records can be used and accessed are being asked in state legislatures and the media. Both of these issues, as well as other aspects of the larger national privacy conversation, are likely to become new pieces of the puzzle for states to solve.

CONCLUSION

Picking up where last session left off, states are working to develop policies that allow for the use of data while safeguarding data privacy in a way that builds public trust that education data can be a powerful tool in supporting learning. Faced with a rapidly changing conversation, an increasing use of education technology in schools, and a shifting national landscape of state and federal laws, state legislators in every part of the country took action this year to better address student data privacy. This national privacy conversation also

remains an opportunity to demonstrate the value of data to improve education. Understanding the concerns and state actions of the past year can help all of us better create policies that effectively safeguard data, support data governance and transparent data decisionmaking, and communicate clearly about how data are used and protected. Ultimately, these policies and practices build public and policymaker trust in the value of data to improve achievement and education opportunities for all students.

³ To help states implement these next steps, EducationCounsel has created a resource articulating the foundational components of a strong student data privacy and security policy and providing model legislative language.

2015 PRIVACY LEGISLATION INDEX

What the bill addressed	Number of bills	Number signed into law
PROHIBITIVE VS. GOVERNANCE APPROACH		
Prohibitive	125	15
Governance	122	24
Both	73	11
SCOPE/TYPE OF DATA		
Collection or sharing of biometric data	22	1
Collection or sharing of school or student education records	11	2
ROLE OF SCHOOL/STATE BOARD		
Privacy-related responsibilities assigned to state boards	35	5
Privacy-related responsibilities assigned to district or county school boards	23	7
ROLE OF SERVICE PROVIDERS AND CONTRACTS		
Data activities of vendors	69	13
Criteria or guidelines for contracts with service providers	61	10
ROLE OF LOCAL EDUCATION AGENCIES		
Privacy or security responsibilities	62	9
REFERENCES TO THE COMMON CORE STATE STANDARDS		
Provisions related to student data privacy and the adoption of state content standards, assessment tools, or curricula or to state participation in assessment consortia	32	2
EMERGENCY BILLS		
Introduced as emergency measures	11	3
DEFUNDING THE STATE LONGITUDINAL DATA SYSTEM		
Prevention of the continued or expanded funding of the state longitudinal data system	11	0
OPT-OUT		
Parental opt-out of data collection or the submission of personally identifiable information to third-party service providers or consortia	81	13
TRANSFER OF STUDENT DATA OUTSIDE THE STATE		
Prohibited the transfer of student data outside the state in at least some circumstances	20	0*
DATA BREACH NOTIFICATION		
Required the implementation of a breach notification process	31	6
PROVISIONS FROM OKLAHOMA HB 1989		
Adoption of many of the provisions outlined in 2014's Oklahoma HB 1989	14	3
PROVISIONS FROM CALIFORNIA'S SOPIPA LAW		
Adoption of many of the provisions of California's 2014 SOPIPA law	44	10

*Note: Louisiana enacted these prohibitions in 2014 and did not alter them in a 2015 amendment to the law.



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

Washington, DC | Phone: 202.393.4372 | info@dataqualitycampaign.org