




State Student Data Privacy Legislation

What Happened in 2014, and What Is Next?


EXECUTIVE SUMMARY


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 have sparked conversation on 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 educators and policymakers alike have begun to develop and implement new policies and practices.


To address emerging concerns, new demands for student data, and increasing use of technology in classrooms, states introduced and passed an unprecedented number of bills addressing student data privacy in 2014.

-  **Thirty-six of the 46 states with legislative sessions in 2014 introduced student data privacy bills.**
-  **One hundred ten bills explicitly addressing the safeguarding of education data were considered.**
-  **Twenty states passed 28 student data privacy bills into law.¹**

These 110 bills represent diverse approaches to safeguarding privacy.

-  **Many bills reiterated existing protections stipulated in the Family Educational Rights and Privacy Act.**

-  **Many bills adopted a narrow focus (such as bills that address only biometric data or social media); broader bills were usually focused on data governance.**

-  **No state defunded its statewide longitudinal data system or halted the linkage of student data across the P-20/workforce systems.**

By summarizing the activity of this legislative session with regard to student data privacy, we can better understand the concerns and issues that drove privacy legislation and shaped its content. We can also begin to understand what the activities and discussions of this year may mean for the next session and for how schools, districts, and states can ensure that privacy safeguards are a critical component of education data use.

For more information on any of the bills or analyses in this paper, contact Rachel Anderson at rachel@dataqualitycampaign.org.

¹ As of August 27, 2014, two California student data privacy bills have passed in the senate and assembly and have been sent to the governor for review. SB 1177 seeks to prevent the commercialization of student data by online service providers while permitting educational activities. AB 1584 seeks to govern how a district can contract with an online service provider for the digital storage and management of education data.



SUMMARY AND ANALYSIS

EVOLUTION OF THE PRIVACY CONVERSATION

Safeguarding privacy is a critical component of effective data use and has been a priority of the Data Quality Campaign (DQC) since the campaign's inception. However, privacy has frequently existed at the periphery of the education data use conversation and has often been seen as an issue of compliance with federal laws (namely the Family Educational Rights and Privacy Act [FERPA]) or the sole purview of IT professionals. But the topic moved into the spotlight in early 2013. This shift in focus was precipitated by growing concern both about the appropriate use of and risks of collecting education data, as well as privacy concerns related to data collection and use in almost every area of public life, from the National Security Agency to Target and financial institutions to health care.


This growing 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 or implementing the Partnership for Assessment of Readiness for College and Careers or Smarter Balanced Assessment Consortium tests) or more general concerns about government overreach, the implications of collecting information about individuals, and the activities of online data service providers.





While the privacy conversation was different in every state, many legislators heard similar concerns and questions around common topics, such as the following:

-  What are the existing provisions and scope of federal student privacy laws including FERPA, the Children's Online Privacy Protection Act, and the Pupil Protection Rights Act?
-  What are state longitudinal data systems (SLDS), and how do data move through them and remain safeguarded?

SUMMARY OF INTRODUCED STATE LEGISLATION

Between the start of each state's 2014 session through August 22, 2014, states considered the following bills:



-  **Thirty-six states** considered **110 bills** explicitly addressing student data privacy.

-  What data elements can be and are shared with the US Department of Education?
-  How do data management service providers (such as inBloom) function and safeguard data?
-  What are the differences in the users and uses of data collected by the district and data collected through online services?
-  What are the value and responsibilities of a chief privacy officer (CPO)? While CPOs have been staples of the private sector for years, how do they fit into education data governance?

These areas of opacity plus additional questions about the value of data sparked an unprecedented surge of legislative activity across the country on this important issue. The 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). DQC's analysis shows 79 bills were introduced using this approach.

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 CPO, description of school board and legislature roles), and supports (state leadership) needed to ensure that data are used appropriately. DQC's analysis shows 52 bills were introduced using this approach.


-  Nearly all of the 36 states (**29**) considered numerous bills.
-  States often considered bills articulating different approaches (i.e., governance AND prohibitive approaches).²

² See the 2014 Privacy Legislation Index at the end of this paper for more details on the types of bills introduced and signed into law.


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

SCOPE/TYPE OF DATA ADDRESSED

Most bills referred to “student data” generally or to any “personally identifiable information” (i.e., information that could be used to identify an individual), but some were more specific.

 **Thirty-nine bills** explicitly addressed the collection or sharing of biometric data.

- **Fourteen of these bills** were signed into law, including three that deal solely with biometric data.


 **Sixteen of the 28 total bills** that were signed into law this session prohibited the collection or sharing of “sensitive data.”


- While sensitive data are not a defined term in federal statute, these bills typically pertained to information on religious or political affiliations, sexual behaviors, gun ownership, health, and psychological data.

STATE BOARD ROLES IN LEGISLATION

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


 **Thirty-two introduced bills** (seven of which were signed into law) gave state boards privacy-related responsibilities.

 The most common roles were rulemaking, creating an inventory of the data collected by the state, and implementing and monitoring privacy and security policies.

 State bills that did not charge the state board with a role usually assigned a role to the state legislature or state education agency (SEA).


LOCAL RESPONSIBILITIES

While legislation focused on the state role, many bills also identified the school district as an important actor in safeguarding student data privacy.

 **Twenty-eight state bills** this session charged districts with responsibilities in safeguarding data and ensuring data quality.


REFERENCES TO THE COMMON CORE STATE STANDARDS

Implementation of the Common Core State Standards and state participation in the related assessment consortia became conflated with data collection and data privacy concerns.


 **Twenty-seven bills** included provisions related to student data privacy and the adoption of state content standards, assessment tools, or curricula or to state participation in assessment consortia.

- **Six of these bills** were signed into law.

DEFUNDING THE SLDS OR HALTING CURRENT DATA INITIATIVES


 A small but significant number of introduced bills (**10**) sought to prevent the continued or expanded funding of the SLDS.

- **None of these bills** were signed into law.

 Some bills sought to stop current education data efforts, but nearly all were defeated.

- Colorado, Georgia, Idaho, and West Virginia all introduced very similar bill language to prohibit the SEA from entering into any commitments related to Race to the Top, prohibit the expenditure of funds for most SLDS activities, and limit the collection and sharing of most student and teacher data.
- **No bills** were passed in any of the four states. Colorado, Idaho, and West Virginia all passed bills addressing student privacy through data governance.

OPT-OUT

 **Seventeen bills** described some type of opt-in or opt-out provision for the collection, use, or disclosure of student data.

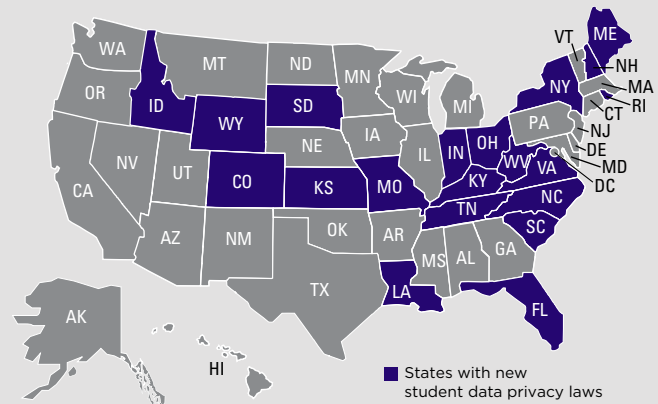
- **Thirteen of these bills** would allow for parents to opt out of data collection, the disclosure of directory information (which is already provided for under federal law), or the submission of personally identifiable information to third-party service providers or consortia.

 Of these 17 bills, **three** were signed into law.

- The passed bills allow district opt-out from the state dashboard or reiterate existing parental opt-out permissions for directory information (an existing provision in FERPA).

SUMMARY OF NEW STATE LAWS

As of August 22, 2014, **28 student data privacy bills** (including four pairs of companion bills) have been signed into law in **20 states**. These 20 states represent a diverse cross-section of the country. The states represent different regions and political environments.







THE NEW PRIVACY LANDSCAPE³


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


DATA GOVERNANCE AND NEW GOVERNANCE BODIES

Some new state laws seek to establish good data governance through the creation of data governance bodies with decisionmaking or investigatory authority. Roles of these bodies include the following:



-  general education data governance and making decisions about data disclosures
-  making data transparent and accessible to the public
-  studying student privacy issues (e.g., with respect to cloud computing services or social media)
-  addressing the concerns of parents about data use

MINIMAL DATA PROHIBITIONS

-  Many bills codified existing practices or reiterated existing prohibitions and do not disrupt the state's current data initiatives.

-  Louisiana passed a bill that requires school districts to obtain parental consent to share personally identifiable information with the state or any other entity. This new law could compromise the state's ability to leverage student data to improve student achievement (e.g., potentially affecting eligibility determination for scholarships and other programs and supports).


ROLE OF SERVICE PROVIDERS AND CONTRACTS

-  Twelve new state laws explicitly govern the permissible activities of online service providers (one of these applies only to contracted testing entities).
-  These laws describe specific requirements for state or district contracts with service providers. These requirements range from general privacy and security acknowledgments to more specific criteria touching on encryption, audits, and breach notification.

³ For more information on each of the new laws, see www.ferpasherpa.org.

NEXT STEPS/NEXT SESSION⁴

As the 2014 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. Strategies states are likely to take in the future include the following:

-  **Introduce bills that build on the provisions established this year and/or rectify unintended consequences created by previous bills** (e.g., clarifying provisions prohibiting the collection of behavior data to provide some flexibility particularly with regard to special education or ensuring that provisions designed to govern the collection of data from students' use of online services does not disrupt the legitimate use of education technologies).
-  **Hold more informational hearings** to gather information on education data topics and engage advocates, experts, educators, and parents.
-  **Adopt a broader approach to governance and transparency to expand the role of parents.** As states and districts acknowledge the critical rights of parents, initiatives such as parent data dashboards mean that parents may be empowered to play an even larger role in the effective use of data in the future.

-  **Provide resources for districts.** Twenty-eight state bills (and nine new laws) this session charged districts with responsibilities in safeguarding data and ensuring data quality. Additionally, many of these bills describe penalties for districts that do not meet these responsibilities. States must help districts build their capacity by providing supports such as staff data privacy training, model contract language for working with service providers, and privacy and security policy language.
-  **Use legislation to better define and govern different categories of data** (i.e., data collected by districts vs. data collected through online services).
-  **Understand existing legislation addressing the commercial uses of data** (including the differences between service providers using data for marketing and using data to improve the quality of and user satisfaction with their product) and expanding protections if needed.

CONCLUSION

Faced with a rapidly changing conversation, an increasing use of education technology, and strong public concern, state legislators in every part of the country took action this year to better address student data privacy. While some new state laws may disrupt aspects of state and local data work, no state has defunded its data system, delinked its data, or stopped critical data services. But privacy concerns and misconceptions still abound, and the 2015 legislative sessions will be just as critical as this year's. However, 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 harness this opportunity and 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.

⁴ 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.

2014 PRIVACY LEGISLATION INDEX

What the bill addressed	Number of bills	Number signed into law
DEFUNDING THE SLDS OR HALTING CURRENT DATA INITIATIVES		
Prevention of the continued or expanded funding of the SLDS	10	0
EMERGENCY BILLS		
Introduced as emergency measures	6	1
LOCAL RESPONSIBILITIES		
Privacy or security responsibilities assigned to school districts	28	9
NOTIFICATION PROCEDURES FOR STUDENT DATA BREACHES		
Implementation of a breach notification process	47	13
OPT-OUT		
Parental opt-out of data collection or the submission of personally identifiable information to third-party service providers or consortia	12	0
Parental opt-out of the disclosure of directory information	1	1
District-level opt-out of submission of student data to the state data portal	3	2
PROHIBITIVE VS. GOVERNANCE APPROACH		
Prohibitive	79	20
Governance or transparency	52	15
Both	26	7
PROVISIONS FROM OKLAHOMA HB 1989 FROM 2013		
Adoption of many of the provisions outlined in Oklahoma HB 1989 from 2013	14	5
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	27	6
ROLE OF SERVICE PROVIDERS AND CONTRACTS		
Data activities of vendors	39	12
Criteria or guidelines for contracts with service providers	64	12
SCHOOL/STATE BOARD ROLES IN LEGISLATION		
Privacy-related responsibilities assigned to state boards	32	7
Privacy-related responsibilities assigned to district or county school boards	11	1
SCOPE/TYPE OF DATA		
Collection or sharing of biometric data	39	14
Collection or sharing of sensitive data as defined by the state	48	16
Collection or sharing of school or student education records	42	8
Collection or sharing of service use-generated data including affective computing	17	1
TRANSFER OF STUDENT DATA OUTSIDE THE STATE		
Prohibited the transfer of student data outside the state in at least some circumstances	26	3



The Data Quality Campaign (DQC) is a nonprofit, nonpartisan, national advocacy organization committed to realizing an education system in which all stakeholders—from parents to policymakers—are empowered with high quality data from early childhood, K-12, postsecondary, and workforce systems. To achieve this vision, DQC supports policymakers and other key leaders to promote effective data use to ensure students graduate from high school prepared for success in college and the workplace. For more information, visit www.dataqualitycampaign.org.