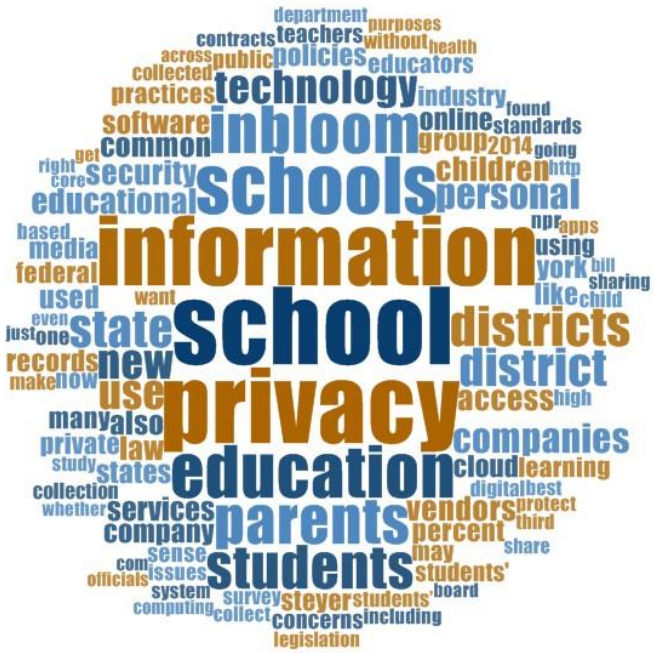
REPORT TO THE STUDENT DATA PRIVACY WORK GROUP



Prepared by the Oregon Education Investment Board (OEIB)

Policy and Research Team

Table of Contents

INTRODUCTION 2

NATIONAL CONTEXT 2

CRITICAL QUESTIONS 3

EXAMPLES OF BEST PRACTICES/GUIDELINES FOR STUDENT DATA PRIVACY 4

THIRD-PARTY VENDORS AND CLOUD COMPUTING SERVICES 4
DEVELOPING STUDENT DATA PRIVACY POLICY 5

APPENDIX 1 - CURRENT KEY FEDERAL DATA PRIVACY PROTECTION LAWS 7

APPENDIX 2 - CURRENT OREGON STATUTES AND ADMINISTRATIVE RULES ON STUDENT DATA PRIVACY 8

APPENDIX 4 - RECENT BREACHES OF STUDENT DATA IN OREGON 9

APPENDIX 5 - LEGISLATIONS AND PRACTICES IN OTHER STATES ON SAFEGUARDING STUDENT DATA 11

REFERENCES 99

Introduction

The Oregon Education Investment Board and Legislative Representatives have convened a workgroup with the intended goal of researching student data privacy issues, analyzing and determining acceptable data use, and writing a policy recommendation with suggested new legislation for the 2015 Legislative Session. This document is a review of the current national discussion of this topic, an identification of key current questions for Oregon, a list of possible suggestions for states to pursue in order to improve their student data privacy policies, and a set of appendices that contain supplementary information necessary for the workgroup. Because the workgroup includes content-area experts from inside and outside the public education system, new research and exemplar practices and policies will likely be brought to meetings and ultimately included in this evolving document.

National Context

At the same time that Oregon is grappling with student data privacy questions and issues, the Federal government is considering the same questions. Amid growing concerns about the security of student data, Sens. Ed Markey and Orrin Hatch have introduced a bill updating the Family Educational Rights and Privacy Act of 1974. The bipartisan bill declares that school districts must meet new rules for protecting privacy in order to receive education funds. It prohibits the use of personally identifiable information to target advertising to students, requires districts to minimize distribution of identifiable data and mandates that any company or organization receiving the data have comprehensive security policies in place.

President Barrack Obama recently pledged billions of dollars supporting the use of technologies in education in the school system (Bidwell, 2014). At the same time, concerns about privacy issues involving student data and technologies have been featured frequently in national media, especially following news like the large scale security breach (Svitek & Anderson, 2014), potential misuse of student data with third-party vendors, and overwhelming concern about advertisers using personal data to market to school children (Common Sense Media, 2014). Many entities are responding to these concerns, including the President's Council of Advisors on Science and Technology (PCAST) with a report titled "Big Data and Privacy: A Technological Perspective". The Common Sense Media, a non-profit organization that evaluates media and educational technology for use by children, recently convened key stakeholders and policy makers at the School Privacy Zone Summit to discuss the issues of legitimate use, storage, and reporting of student data. Many states, including Colorado, Kansas, Idaho, Tennessee, California, Oklahoma and Massachusetts, have

joined the movement to establish clear and transparent policies and procedures for governing student data in educational settings.

An analysis of popular media (e.g. Washington Post, Huffington Post, Education Week, New York Times, etc.) focused on student privacy issues, identified a set of common concerns about the way data in educational settings nationwide are collected, stored, and reported which have emerged consistently over time and across the country. The graphic on the cover of this document depicts the words most commonly used in these articles. One consistent theme from this collection reflected overwhelming concerns about the use of student data for non-education purposes by third-party vendors (Singer, 2013a, 2013b; 2014c; Herold, 2014b; Hensley-Clancy, 2013; Gilbertson, 2014; Kamisar, 2014; Nagel, 2014; Molnar, 2014; Osborne, 2014; Resmovits, 2014; Vacar, 2014). Third-party vendors offering technology services (e.g. InBloom) gain access to student data because they are contracted by educational institutions to store and manage large student data sets. Current laws, policies, and procedures on protecting student data at the federal, state, district, and institutional levels have not been able to keep up with the growing technological trends (Hensley-Clancy, 2013) and leave room for multiple interpretations (Rice, 2014). Consequently, many are calling for new regulations to protect student privacy that are more transparent (Lu, 2013; Molnar, 2014; Osborne, 2014; Resmovits, 2014; Singer, 2013b, 2014c).

Additional concerns may also warrant further legislative considerations, such as “the use of location data, biometric data, and social media to track students; the metadata generated by students' digital devices, especially when they are used outside of schools; and the growing trend of merging the "learning path" information generated by digital instructional materials with the personal data contained in student profiles” (Kamisar, 2014). Given that the ever-changing nature of the technological landscape will present new privacy issues in the near future, it is important to keep in mind that any policies, procedures, and legislations crafted now may need to take into account future technological advancements, environmental trends, and behavioral factors. Other concerns about data security include the potential for “surveillance” of students through massive data collection (Singer, 2013a), the ability to conduct data-mining and analysis (Lawrence, 2013; Kamisar, 2014; Singer, 2013a, 2014c), and the potential for information being accessible to individuals with criminal intentions (Lawrence, 2013; Lu, 2013).

Critical Questions

Privacy concerns are rising at the same time that schools, districts, and educational agencies are working to increase and improve internal use of student-level data to

improve student outcomes. This context has led to specific current issues where new questions are being raised about student data privacy and acceptable use. These areas of discussion/debate include:

- Implementation of the Common Core State Standards (CCSS) and the Smarter Balanced Assessment Consortium (SBAC)
- Oregon's student-level data collection and sharing practices
- Types of data collection activities associated with the Statewide Longitudinal Data Systems (SLDS) grant program, the American Recovery and Reinvestment Act (ARRA), and Race to the Top
- The pros and cons of centralizing the collection and storage of student information
- The ways in which Family Educational Rights and Privacy Act (FERPA) attends to student privacy protection (See Appendix 1)
- The overlap between FERPA and Oregon laws protecting student privacy
- Vendor and corporation access to student-level data for non-educational purposes

Examples of Best Practices/Guidelines for Student Data Privacy

In response to the growing concerns about student data security, the U.S. Department of Education established the Privacy and Technical Assistance Center (PTAC), as a one-stop shop to provide comprehensive information on data privacy, confidentiality, and security practices related to uses of student data, including student-level longitudinal data. PTAC also focuses on providing education stakeholders the latest publication on student privacy, confidentiality, and security practices through training videos and direct assistance (for details, see http://ptac.ed.gov/).

Third-party Vendors and Cloud Computing Services

A quick online search on the words "cloud" and "education" yielded 301,000,000 results in .49 seconds. "Cloud" and associated terms like "cloud-technologies" and "cloud-based educational technologies", are often tied with many current student privacy issues. According to the National Institute of Standards and Technology (NIST), "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011, p. 2). The adoption of cloud computing services in educational institutions is widespread, with 95% of school districts (K-12) in a nationally representative sample currently using one or more forms of cloud-based educational technologies (Reidenberg, Russell, Kovnot,

Norton, Cloutier & Alvarado, 2013). Given the high rate adoption rate of cloud-based technologies, several policy guides have been created by policy and research organizations to assist educational agencies and institutions that are considering using cloud-computing solutions for education data. For example, PTAC issued a "frequently-asked-questions" document in 2006 and is equipped with answers to questions about meeting necessary data privacy and data security requirements, including compliance with the FERPA, to ensure proper protection of education records (for details, see http://ptac.ed.gov/sites/default/files/cloud-computing.pdf).

The National School Boards Association (NSBA, 2014) recently published a policy guide titled "Data in the Cloud: A Legal and Policy Guide for School Boards on Student Data Privacy in the Cloud Computing Era". This document provides relevant terminology, current academic research, software programs, legal requirements, and fundamental resources for board members and lawyers in school districts.

The Berkman Center for Internet & Society, a research center that focuses on the development, dynamics, norms, and standards of cyberspace, also contributed on cloud computing services discussion by starting the Student Privacy Initiative as an avenue for stakeholders from government, educational institutions, academia, and businesses, to discuss the pros and cons of using cloud computing services in educational institutions. This initiative has already produced a guide titled "Framing the Law & Policy Picture: A Snapshot of K-12 Cloud-Based Ed Tech & Student Privacy in Early 2014". This guide targets policy makers at the school district, local, state and federal government levels and recommended the following guides based on the current state of cloud computing services (see details in Plunkett, Solow-Niederman & Gasser, 2014):

- Employing temporary centralization of cloud-based educational technologies (ed tech) decision-making at the district level to foster the legal, technical, and other expert oversight necessary in this complex space without stifling capacity for local experimentation
- Examining the adoption of user-friendly labeling of cloud-based ed tech products to increase transparency and encourage compliance with parental consent and other legal requirements
- Adopting FIPPs (Fair Information Practice Principles) and other best practice standards by industry providers to increase data security and protection

Developing Student Data Privacy Policy

Many other organizations have contributed to student data privacy policy by publishing guidance on student data protection at the legislative level. The American Legislative Exchange Council (ALEC), a non-profit organization that publishes and conducts research on state-based public policy issues, also provided state-level guidance by

proposing a model policy titled “The Student Data Accessibility, Transparency, and Accountability Act”. This model was adapted from the Oklahoma House Bill 1989 (Lu, 2013, Data Quality Campaign, 2013). The model encourages policy makers to do the following:

- to prepare, inventory and index of all data elements with definitions of individual student data fields currently in the statewide longitudinal data system
- to create a data security plan, ensuring compliance with federal and state data privacy laws and policies
- to ensure contracts with third-party vendors to include privacy and security provisions
- to create a Chief Privacy Officer (CPO) at the state-level to ensure department-wide compliance with all privacy laws and regulations (Source: http://www.alec.org/model-legislation/student-data-accessibility-transparency-accountability-act/)

The Software & Information Industry Association (SIIA), a Washington-based trade group, developed a document titled “Policy Guidelines for Building a Student Privacy Trust Framework” (2014). Mark Schneiderman, Senior Director of Education Policy at SIIA, presented key elements of this document to the California State Assembly’s Joint Hearing of the Committee on Education and the Select Committee on Privacy On Ensuring Student Privacy in the Digital Age in May, 2014. SIIA advocated for industry self-regulation and listed these areas of guidance:

- to define the educational purpose in collecting students' personally identifiable information (PII) from schools
- to promote transparency in the types and reasons for collecting PII
- to establish an agreement that PII be collected and used only as authorized by schools or required by law
- to design security policies and practices be used for what is collected
- to establish data-breach notification policies and procedures to be in place.

Appendix 1 - Current Key Federal Data Privacy Protection Laws

The **Family Educational Rights and Privacy Act** (**FERPA**) is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education (see http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html for details).

Other applicable federal laws include:

1. **Children's Online Privacy Protection Act** (**COPPA**) -- imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age (see http://www.coppa.org/coppa.htm)
2. **Children's Internet Protection Act** (**CIPA**) -- address concerns about children's access to obscene or harmful content over the Internet (see http://www.fcc.gov/guides/childrens-internet-protection-act)
3. **Protection of Pupil Rights Amendment** (**PPRA**) - protects the rights of parents and students on:
    - Any material used by students in U.S. Department of Education funded surveys, analyses, or evaluations will be made available to parents to inspect prior to use with their child
    - Ensures that schools and contractors acquire written parental consent before a minor student is required to participate in U.S. Department of Education funded surveys, analyses or evaluations which may reveal personal information concerning:
        - Political affiliations;
        - Mental and psychological problems potentially embarrassing to the student and his/her family;
        - Sex behavior and attitudes;
        - Illegal, anti-social, self-incriminating and demeaning behavior;
        - Critical appraisals of other individuals with whom respondents have close family relationships;
        - Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers; or
        - Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program)
        - See http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

Appendix 2 - Current Oregon Statutes and Administrative Rules on Student Data Privacy

Oregon's privacy laws and practices on education data are governed by the following Oregon revised statutes (ORS), Oregon Administrative Rules (ORA), and the Department of Administrative Services (DAS):

Number	Title	Effective Date
ORS 646A.600 – 626	Oregon Revised Statute – Oregon Consumer Identity Theft Protection Act	2007
ORS 182.122	Oregon Revised Statute – Information systems security in executive department; rules	2005
ORS 291.038	Oregon Revised Statute – State agency planning, acquisition, installation and use of information and telecommunications technology; integrated videoconferencing; online access service; Stakeholders Advisory Committee; rules	2003
ORS 184.305	Oregon Revised Statute – Purpose and authority of the Oregon Department of Administrative Services to provide centralized services, provide rules and oversight of policy compliance by agencies, etc.	1993
ORS 291.037	Oregon Revised Statute – Legislative findings on information resources identifying that information is a strategic asset of the state and allowing for centralized establishment of rules and standards for information management.	1991
OAR 125-800-0005	Oregon Administrative Rule, Division 800, State Information Security – Purpose, Application, and Authority	12/28/2006
OAR 125-800-0010	Oregon Administrative Rule, Division 800, State Information Security – Definitions	12/28/2006
OAR 125-800-0020	Oregon Administrative Rule, Division 800, State Information Security – State Information Security	12/28/2006
DAS 107-004-110	DAS* Statewide Policy – Acceptable Use of State Information Assets	1/1/2010
DAS 107-004-053	DAS Statewide Policy – Employee Security	7/30/2007

Note. *ORS 182.122 (House Bill 3145, 2005 Legislative Session) designates DAS as the "single point of accountability" for information security at the state. In support of this mandate, the Enterprise Security Office (ESO) is instituting a security strategy wherein DAS works collaboratively with state agencies to ensure the state's security posture is at an acceptable level. Information security management enables information to be shared while ensuring protection of that information and its associated technology assets.

Appendix 4 - Recent Breaches of Student Data in Oregon

Since 2007, eight cases of student data breaches were reported in several educational institutions in Oregon:

Year	Month	Institution	Type	Description	# Records
2008	Jun	Oregon State University	HACK	The Oregon State Police are investigating the theft of personal information from online customers of the OSU Bookstore who used credit cards to purchase items. *Information Source: Dataloss DB.*	4700
	Dec	Oregon Health and Science University	PORT	A laptop stolen in Chicago contained health records. It was stolen from a hotel while an OHSU employee was there on business. The data could include medical record numbers, names, telephone numbers, dates of birth, gender, Social Security numbers, addresses, medical diagnosis category and category of treatment - but not the specific treatments. *Information Source: Dataloss DB.*	890
2009	Jan	University of Oregon	PORT	A laptop computer containing data files for Youth Transition Program (YTP) participants was stolen. Those files contained names and social security numbers. *Information Source: Dataloss DB.*	(Not Reported)
	Jan	Southwestern Oregon Comm. College	PORT	A laptop computer was stolen from the campus putting former and current students at risk. *Information Source: Dataloss DB.*	200
	Mar	Pacific University	PORT	Student Life (503) 352-2212, Faculty and staff (503) 352-1511, Legal Affairs (503) 352-2236 A University-owned laptop was stolen from a staff member's residence. The stolen laptop was password protected and there is no factual evidence that any private information was stored on the laptop. The computer contained names and some personal information. It does not appear that any Social Security numbers were stored on the system. *Information Source: Dataloss DB.*	0
2011	Jan	Warner Pacific College	PORT	A laptop was stolen from an employee's home on January 3. It contained the names, Social Security numbers, dates of birth, telephone numbers and addresses of students. *Information Source: Media.*	1,536
2012	Jun	Eugene School District 4J	HACK	An unauthorized person accessed confidential files that contained current and former students' personal information. Names, Social Security numbers, Dates of birth, student ID numbers, phone numbers, students' free or reduced-price school	16,000

			lunch status, and addresses may have been exposed. UPDATE (07/12/2012): A minor was arrested for possible involvement in the breach. It appears that the teenager may have obtained the login credentials of an employee and used them to access the computer system. Records for approximately 16,000 current students, as well as free and reduced-price lunch records from 2007 were exposed. UPDATE (08/25/2012): The student was released from custody and expelled by North Eugene High School. He also posted hundreds of students' confidential information on a computer account to taunt district officials. He is on house arrest and his attorney entered not guilty pleas. *Information Source: Databreaches.net*	
Jul	Oregon State University	INSD	An unnamed check printing vendor for the University copied data from the University's cashier's office during software upgrades. The information included 30,000 to 40,000 checks that contained student and employee names, University IDs, check numbers, and check amounts. Current and former student, faculty, and staff records older than 2004 may have included Social Security numbers. it does not appear that the vendor acted with malicious intent. *Information Source: Media*	21,000

Note. HACK - Electronic entry by an outside party, malware and spyware; PORT - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.; INSD - Someone with legitimate access intentionally breaches information - such as an employee or contractor; Total of 570 breaches in the U.S. from 2007 to present in educational institutions. Statistics retrieved from https://www.privacyrights.org/data-breach/

Appendix 5 - Legislations and Practices in Other States on Safeguarding Student Data

Listed below are legislations in other states on protecting student data (provided by Reg Leichty, Partner, EducationCounsel).

State	Bill Number	Bill Title	Summary	Date of Introduction	Status	The bill is prohibitive	The bill provides for transparency, governance, and/or accountability	The bill would move the state backwards on DQC's 10 elements/ actions	Notes
Alabama	HB 569	Student data, use of by providers of cloud computing service	This bill would prohibit K-12 cloud computing service providers from using student data for any secondary purpose that may benefit the cloud computing service provider or a third party for commercial purposes. [Note: This is the House version of SB 425 below]	3/4/2014	Introduced	Yes	No	No	This bill reiterates existing prohibitions and does not describe any governance efforts.
Alabama	SB 425	Student data, use of by providers of cloud computing service	This bill would prohibit K-12 cloud computing service providers from using student data for any secondary purpose that may benefit the cloud computing service provider or a third party for commercial purposes. [Note: This is the Senate version of	3/4/2014	Introduced	Yes	No	No	This bill reiterates existing prohibitions and does not describe any

			HB 569 above]						governance efforts.
Alaska	HB 257	An Act relating to restrictions on the collection, storage, and handling of student data.	This bill would require the state DOE to report to the legislature annually on changes made to the collection of student data and the results of annual security audits. The bill would also require the board to create a data inventory of the student data collected, its purpose, who has access, location of storage server, nongovernmental entities with access, and a description of safeguards, a policies to limit access and reasons for data access and transfer. The bill would also prohibit the collection of biometric data and other data such as medical or religious data. Finally, the bill prohibits the sharing of student data including email addresses for marketing purposes.	1/21/2014	Introduced	Yes	Yes	No	This bill provides for security audits and a public data inventory, but also prohibits the collection of some types of data and limits access to data.
Arizona	HB 2702	Cloud Computing Services; Student Privacy	This bill would prohibit cloud computing service providers from using student data for any secondary purpose that benefits the provider or another third party. The bill would require that	2/17/2014	Introduced	Yes	No	No	This bill reiterates existing prohibitons and does not

			any educational institution working with a service provider document this prohibition in writing.						describe any governance efforts.
Arizona	HB 2645	Ade; Education Data System; Privacy	This bill would require a public data inventory (including collected elements, definitions, and purposes), a public notice and comment period for new data elements, an annual report on data collection and the results of security audits. The bill also requires the Department to create a data request approval process and ensure role-based access for specific purposes. The bill creates a CPO position and ensures processes for public complaints and the investigation of any security incidents. The bill also calls for transparency around the state's privacy policy and data communications.	2/10/2014	Passed in the Senate	No	Yes	No	This bill describes governance and data privacy protections without being prohibitive. This bill adopts many of the provisions outlined in OK HB 1989.

Arizona	HB 2316	An act relating to local education control and student privacy.	This bill would require that student data must be collected in ways that conform to state and federal privacy laws. The bill would also prevent the sharing of PII with the federal government or with vendors for the purpose of marketing with respect to religious, political, psychometric, or standardized test information on the student or their family.	1/17/2014	Vetoed	Yes	No	No	This bill reiterates existing prohibitons and does not describe any governance efforts.
California	AB 1584	An act to add Section 49073.1 to the Education Code, relating to pupil records.	This bill would authorize a local educational agency to enter into a contract with a third party to provide services for the digital storage, management of education data. The bill would require the contract to specify that the LEA owns and controls the data, how the third party will secure the records, how and the LEA and the third party will jointly ensure compliance with specified federal privacy acts.	2/3/2014	Introduced	No	Yes	No	This bill seeks to govern data and use of third parties effectively without being prohibitive.
California	SB 1177	Privacy: students.	This bill would prohibit an online K-12 service provider from selling or use of student data for marketing purposes (but permits program improvement).	2/20/2014	Passed in the Senate	Yes	No	No	This bill limits the selling of student data but does not describe governance

									measures.
Colorado	SB 204	Education Data Privacy And Security Act	This bill require parental consent for the collection of some data (some medical data, some workforce data, biometric records, data collected from affective computing, psychological data, and religious affiliation). The bill would also require parental consent for predictive analytics and would prohibit funding for any state data system that does not follow these limitations. The bill would prohibit interagency data sharing and limit interstate sharing. The bill would require a public inventory of all PII collected and public notification of the data collections' authorizing body, expected disclosures, contracting policies with third parties, and a contact point. The bill would also require each state agency or educational institution to report any new proposed data collections or changes to data collections to the governor, state assembly, and state board. The bill would limit the disclosure of PII for research	4/16/2014	Introduced	Yes	Yes	Yes	Limiting the collection, use, and disclosure of education data for legitimate education purposes renders most of the DQC state actions impossible. This bill prohibits the collection and use of education data while also

			purposes, limit the sharing of data with third parties not fulfilling specific duties, and prohibit third parties from using data for commercial gain. The bill requires certain security protections and a security audit. Finally, the bill would also prohibit the use of assessments that collect psychological or sensitive data and would limit the types of data that could be shared with an any consortia.						providing some governance measures.
Colorado	HB 1294	CONCERNING STUDENT DATA COLLECTION PRIVACY PROTECTIONS ADMINISTERED BY THE DEPARTMENT OF EDUCATION.	This bill provides definitions of key terms and would provide for a public data inventory, staff training, breach notification, contracting guidelines, and describes permissible uses of education data.	2/26/2014	Signed into law	No	Yes	No	This bill seeks to govern data effectively without being prohibitive.

									This bill adopts many of the provisions outlined in OK HB 1989.
Delaware	SB 269	AN ACT TO AMEND TITLE 14 OF THE DELAWARE CODE RELATING TO COMMON CORE.	This bill would prohibit the state from implementing the Common Core State Standards and participating in any assessment consortia or Race to the Top activities. The bill would prohibit the spending of any funds on any SLDS beyond what is needed for basic administration and federal compliance activities. The bill would prohibit the sharing of any PII outside of the state except for federal requirements. The bill would prohibit the sharing of PII with any entity for the development of commercial products or for economic or workforce development planning.	7/1/2014	Introduced	Yes	No	Yes	Defunding of the SLDS is in direct opposition to DQC data elements and would render most state actions impossible. Much of this bill deals with Common Core and state standards control.

Florida	HB 195	An act relating to education data privacy	This bill would require annual notice of education record rights for parents and students, limit the collection of student data including biometric, religious, or political information. The bill would also limit the disclosure of information to repsonding to a subpoena and requires agency or institutions to reguarly consider whether the disclosure of directory ionformaiton as defined in FERPA would place students at risk for marketing campaigns. The bill would also require students to present documentation of their SSN upon enrolling in school; the state would then assign a different student ID. [Note: This is the House version of SB 188 below]	2/11/2014	Signed into law (as SB 188)	Yes	No	Yes	This bill was originally introduced in 2013 with a prohibitive, biometric data focus, but was rewritten as a general privacy bill in Feb, 2014. This bill prohibits the disclosure of data in such a way that directly compromises the DQC 10 state actions without

									describing any governance measures.
Florida	SB 188	An act relating to education data privacy	This bill would require annual notice of education record rights for parents and students, limit the collection of student data including biometric, religious, or political information. The bill would also limit the disclosure of information to repsonding to a subpoena and requires agency or institutions to reguarly consider whether the disclosure of directory ionformaiton as defined in FERPA would place students at risk for marketing campaigns. The bill would also require students to present documentation of their SSN upon enrolling in school; the state would then assign a different	2/10/2014	Signed into law	Yes	No	Yes	This bill was originally introduced in 2013 with a prohibitive, biometric data focus, but was rewritten as a general privacy bill in Feb, 2014.

			student ID. [Note that this is the Senate version of HB 195 above]						This bill prohibits the disclosure of data in such a way that directly compromises the DQC 10 state actions without describing any governance measures.
Florida	SB 232	Biometric Information; Prohibiting a school district or school from collecting a student's biometric information, etc.	This bill defines biometric data and forbids any school or district from collecting biometric data.	10/3/2013	Introduced	Yes	No	No	This bill was introduced in 2013, but remains technically active.

Georgia	SB 167	Education; declare certain actions void ab initio relating to adoption of certain curricula	This bill would halt the adoption Common Core State Standards, prohibit the SEA from entering into any commitments related to Race to the Top, and would prohibit the expenditure of funds for an SLDS beyond what is needed for administrative needs and federal grant compliance. The bill would also limit the collection and sharing of student and teacher PII.	2/14/2014	Died in the House after passing in the Senate	Yes	No	Yes	Defunding of the SLDS is in direct opposition to DQC data elements and would render most state actions impossible. Much of this bill deals with Common Core and state standards control.

Idaho	SB 1385	RELATING TO CERTAIN EDUCATIONAL RECORDS AND DATA	This bill would prohibit the disclosure of some student record data, limit the education data that can be collected without consent (including "sensitive information", biometric data, health or psychological data), prohibit the sharing of PII with third parties without consent, prohibit the commercial use of student data, and limit data sharing outside of the state or agency. The bill would ban predictive modeling (except for drop out prevention) and limit video monitoring. The bill would also prevent funding from being used for any data system that tracks students beyond K-12. The bill would also prevent the state from sending any data to an assessment consortium. The bill also calls for data transparency including a public list of collected data elements, research criteria, and processes for breach notification and destruction of data.	3/4/2014	Introduced	Yes	Yes	Yes	Defunding of the SLDS and prohibiting data collection and use are in direct opposition to DQC data elements and would render most state actions impossible. This bill prohibits the use and sharing of data for educational purposes and describes

									some transparency measures.
Idaho	SB 1372	This act shall be known as the "Student Data Accessibility, Transparency and Accountability Act of 2014."	This bill establishes the value of data in the state and calls for an annual education data inventory, the development of data privacy and data collection procedures, and introduces civil penalities for the misuse of data. The bill would also establish provisions relating to data management and analysis contracts. The bill would require parental consent for vendor services. [Note: This bill is similar to SB 1296 below but was introduced into a different committee]	2/27/2014	Signed into law	Yes	Yes	No	This bill seeks to govern data effectively without being prohibitive. This bill adopts many of the provisions outlined

									in OK HB 1989.
Idaho	SB 1296	This act shall be known as the "Student Data Accessibility, Transparency and Accountability Act of 2014."	This bill establishes the value of data in the state and calls for an annual education data inventory, the development of data privacy and data collection procedures, and introduces civil penalities for the misuse of data. The bill would also establish provisions relating to data management and analysis contracts. The bill would require parental consent for vendor services. [Note: This bill is similar to SB 1372 above but was introduced into a different committee]	2/6/2014	Introduced	Yes	Yes	No	This bill seeks to govern data effectively without being prohibitive. This bill adopts many of the provisions outlined in OK HB 1989.

Illinois	SB 3092	EDUC DATA SYSTEM-PERSONAL INFO	This bill would require the State Board of Education or a public school shall designate parties only under its direct control to act as authorized representatives to conduct any audit, evaluation, or activity that is used for enforcement of data access roles. The bill would also limit the disclosure of PII to service providers, parties conducting research for the School Board, or to parties for a commercial use. The bill would also limit the maintenance of PII. Finally, the bill would limit appending education records with PII obtained from other federal or State agencies through data matches. (Note: was amended)	2/7/2014	Passed in the Senate	Yes	No	Yes	This bill limits the maintenance and use of data and does not describe governance measures. Limiting work done through state data matches is in opposition to DQC data elements.

Illinois	HB 4558	SCHOOL STUDENT RECORDS-RELEASE	This bill defines "School Student Record" as including (i) any unique identification number; (ii) any unique user name, other than the student's name itself; and (iii) any other unique information used to identify an individual student. The bill would also provide that school student records or information contained in the records may be released, transferred, or disclosed for evaluation, auditing, reporting, or planning purposes with wittren notice and consent. (Note: was amended)	2/4/2014	Introduced	Yes	No	No	The bill is prohibitive of data sharing (requiring specific notice and consent activities). While parts of the bill describe permitted activities, there is no governance outlined.
Indiana	HB 1003	Economic Development	This bill would establish the Indiana network of knowledge (INK) and describes the composition of the group. This group is charged with data governance and making the state's data accessible (including student progress and outcomes over time, program participation, and employment outcomes).	Reprinted 1/28/2014	Signed into law	No	Yes	No	This bill seeks to govern data (especially high ed and workforce data) effectively without being

									prohibitive.
Indiana	SB 224	Education Standards Chapter 7.5. Student Data Accessibility, Transparency, and Accountability	This bill would require the state board to establish policies and procedures in accordance with FERPA to ensure the confidentiality of student information collected or retained by the department (including auditing and data breach procedures, and data releases). The bill also specificies who can access the student data (including authorized staff, parents, and for reporting purposes), and requires an annual report about the security of student data. The bill would require a public list of collected data elements and proposed new data elements. The bill would prohibit data from leaving the state except under certain circumstances (including data management services from a service provider).	2/7/2014	Introduced	No	Yes	No	This bill seeks to govern data effectively without being prohibitive. Much of the bill gives the state board's authority to adopt state content standards.

Indiana	HB 1320	Act regarding: Student records	This bill would require the state DOE to establish a statewide student record repository to provide for relevant parents and school access, to transfer student records between schools, and to create a backup of student data for schools. This bill would also prohibit an agency from releasing, selling, or otherwise transferring student information to the federal government or another entity unless it is deidentified or the General Assesmbly has passed legislation allowing it.	1/15/2014	Introduced	Yes	No	No	This bill reiterates existing data sharing prohibitions and also provides for the creation of a database.
Indiana	SB 277	Student information. Defines "agency". Sets forth circumstances under which an agency may release student information to a third party.	This bill defines the conditions under which student record can be shared (when a student transfers to a new school or enters a PS institution, for national or multistate assessments, and as allowed by contacts for research or data sharing purposes or with a service provider for data management services).	1/30/2014	Introduced	No	No	No	This bill reiterates existing data sharing permissions and does not describe any governance efforts.

Iowa	HB 2439	A bill for an act relating to core content standards, assessments, and curricula relating to student academic progress, and to the collection of and access to student data.	This bill would require the DOE to establish a data security policy (including breach plans and retention and destruction procedures), a student data privacy policy, and data sharing policies. The bill would also require an annual inventory of the data collected and set up procedures for changing the data elements collected. The bill would limit the sharing of data outside of the state except "as necessary to carry out the duties and responsibilities of the state board or the department." The bill would prohibit the state from collecting biometric, health, or criminal data.	3/5/2014	Introduced	Yes	Yes	No	This bill describes governance and data privacy protections without some limitations on the collection and sharing of data. Much of this bill deals with Common Core and state curriculum control.

Iowa	HB 592	An Act relating to core content standards, assessments, curricula relating to student academic progress, and to the collection of and access to student data.	The bill calls for the establishment of data collection, privacy, and sharing policies. The bill would also require an annual education data inventory and public report and a security plan that addresses data retention and destruction, data breaches, privacy compliance standards, and guidelines for parental access. The bill reads that biometric and other sensitive data will not be included in student records unless provided by another state or federal law.	2/4/2014	Introduced	No	Yes	No	This bill describes governance and data privacy protections without being prohibitive. This bill adopts many of the provisions outlined in OK HB 1989. Much of this bill deals with Common Core and state curriculum control.

Kansas	HB 2621	AN ACT concerning schools	This bill would prohibit the collection of non-cognitive data about students and teachers without writen consent. The bill would also prohibit the DOE or school board from using any funds to support the SLDS or any study beyond what is necessary for administrative functions directly related to the student's academic progress, for evaluation of education programs, or for compliance with federal law. Except in certain circumstances (including contracting with a vendor), the bill would prohibit any student or teacher PII from being sent to any state or local agency in or out of the state, or to any other entity. Finally, the bill would prohibit the use of the Common Core standards and would create an advisory board to determine the state's content standards.	2/11/2014	Died in Committee	Yes	Yes	Yes	Defunding of the SLDS and prohibting data collection are in direct opposition to DQC data elements and would render most state actions impossible. This bill establishes guidelines for working with vendors and making curriculum

									deciusions, but also prohibits the use of data for legitimate education purposes. Much of the bill gives authority to a new advisory group to adopt state content standards in place of CCSS.
Kansas	SB 367	AN ACT concerning schools; creating the student data privacy act	The bill limits defines permissible circumstances for sharing from the SLDS (includes for a department, district, or regents board needing data for their assigned duties, parents/students, or for a data sharing agreement ahereing to privacy and security procedures). The bill would also prohibit the collection of biometric data by school districts and would require	2/10/2014	Signed into law	Yes	Yes	No	This bill restricts the collection of biometric data and also describes governance and

			the state to list the data elements sent to the SLDS.						transparency efforts.
Kentucky	HB 232	AN ACT relating to security breach notifications	This bill would prohibit service providers from using student data for secondary purposes (including for advertising services) without consent.	1/21/2014	Signed into law	Yes	No	No	This bill reiterates existing protections without describing any governance measures. The student data section is one part of a larger bill on general data breach notificatio

									n.
Kentucky	HB 5	AN ACT relating to the safety and security of personal information held by public agencies.	This bill would establish breach notification procedures for data stored by any state agency or any service provider on behalf of a state agency. The bill would require service provider contracts to have strong privacy and security provisions.	1/9/2014	Signed into law	No	Yes	No	This bill establishes data governance around breach notification without being prohibitive.

Kentucky	SB 224	AN ACT relating to public school standards	This bill would prohibit the release of PII as part of a grant process without consent. The bill would require that data collected by the DOE and any contracted service provider is limited to the data needed for their obligations to the district. The bill would require a public listing of all data and web-based service providers used and would require parental consent for any third party provider. The bill would also require that when contracting with service providers, districts retain ownership of their data and that the data be used for the contarcted purpose only. The bill also contains other contract provisions for working with third parties and and governance measures including a guidance document for districts, a requirement for district policies related to cloud service providers, an inventory of PII elements shared with third parties, and a security practice and data minimization review team. Finally, the bill says "Parents have a maximum amount of flexibility to opt out of providing data beyond the minimum necessary and are fully briefed on those rights."	3/6/2014	Introduced	Yes	Yes	No	This bill establishes guidelines for working with vendors and describes governance measures while also limiting the sharing of data for education purposes. Much of this bill deals with Common Core and state curriculum and content standard control.

Kentucky	HB 547	AN ACT relating to education rights and privacy	This bill would require the DOE and all school districts to adhere to transparency and privacy standards for outsourcing Web-based tasks to vendors. The bill would call for contracts to align with FERPA, describe when and how PII needs to be released, describe the obligations of the contractor to de-identify the data, and have any employees and subcontractors agree to confidentiality and nondisclosure.	3/4/2014	Introduced	No	Yes	No	This bill seeks to provide governance and transparency and around contracting with vendors without limiting the appropriate use of data.
Kentucky	SB 89	AN ACT relating to public school standards	This bill would direct the Kentucky Board of Education to require that the DOE and all districts adhere to transparency and privacy standards when outsourcing to vendors (including provisions for data breaches, data redisclosure, prohibitions on the use of data for marketing, and parental access). The bill also clarifies vendor contract requirements and would require districts to publicly list the third-party web-based services they use. Schools would have to notify parents about the data sent to these providers.	2/6/2014	Passed in the Senate	No	Yes	No	This bill seeks to increase transparency and establish some governance around contracting with vendors. Much of the bill focuses

									on other topics including permiting a local board or school council to supplement the state board-approved academic content standards.
Louisiana	HB 946 (became HB 1076)	STUDENTS: Provides for limitations and prohibitions on the collection and sharing of student information and provides penalties for violations	This bill would limit the PII data that could be included in a student's cumulative record, and would prohibit sending student PII to the state. The bill would prohibit service providers from having access to a public computer system where student information is stored without written consent.	2/28/2014	Signed into law	Yes	No	Yes	Prohibiting the submission of student PII to the state is in direct opposition to DQC data elements and would render most

									state actions impossible. The bill lists numerous prohibitions on educational uses of data without describing any governance measures.
Louisiana	HB 340	PERSONAL ONLINE ACCOUNT PRIVACY PROTECTION ACT	This bill would prohibit educational institutions from requesting or requiring the disclosure of information (password, username) that would allow access to personal online accounts except if the device or account is provided by the school or if the information is in the public domain.	3/10/2014	Signed into law	Yes	No	No	This bill is prohibitive, but very narrowly and does not apply to school-owned devices or educational accounts.

									This bill mainly focuses on prohibiting employers from requiring their employees password.
Louisiana	HB 1283	AN ACT To enact R.S. 17:3913, relative to the transfer of personal student information by local education agencies and the state Department of Education	This bill would require the state Department of education and local education agencies to publish on their websites information about how student PII are transferred. The posting would include: 1. a profile of each PII recipient; 2. a copy of the data sharing agreement; 3. a list of the data elements to be transfered; 4. a statement on the intended use of the data; 5. contact information for a person available for public questions; 6. a process for parents to register a complaint.	5/14/2014	Signed into law	No	Yes	No	This bill seeks to provide transparency around data transfers without being prohibitive.

Louisiana	SB 536 (became SB 685)	SCHOOLS. Provides for K-12 student data privacy	The bill would require a public data inventory, transparency around data use and access, a security plan, annual reporting and state board rules. The bill also limits the sharing of PII to federal, state, or local agencies or organizations but provides exceptions for contracted service providers.	2/28/2014	Introduced	No	Yes	No	This bill describes governance and data privacy protections without being prohibitive.
Louisiana	SB 455	STUDENTS. Provides for limitations and prohibitions on the collection and sharing of student information.	This bill would limit local and state collection and use of student data to basic contact information and would prohibit the collection of PII.	2/28/2014	Introduced	Yes	No	Yes	Prohibiting the collection of all PII is in direct opposition to DQC data elements and would render most state actions impossible.

Louisiana	HB 384	STUDENTS: Provides for limitations and prohibitions on the collection and sharing of student information and the administration of assessments, surveys, and other instruments that solicit certain student information	This bill would limit local and state collection and use of student data to basic contact information and would prohibit the collection of PII. This bill would prevent the state and districts from adopting any assessment that collects noncognitive data about students or their families. The bill would limit the sharing of data with assessment consortium to aggregate data and impose other conditions.	2/25/2014	Introduced	Yes	No	Yes	Prohibiting the collection of all PII is in direct opposition to DQC data elements and would render most state actions impossible. Much of this bill deals with Common Core and the state's curriculum.

Louisiana	HB 378	STUDENTS: Provides for limitations and prohibitions on the collection and sharing of student information and provides penalties for violations	This bill would limit local and state collection and use of student data to basic contact information and would prohibit the collection of any PII.	2/25/2014	Introduced	Yes	No	Yes	Prohibiting the collection of all PII is in direct opposition to DQC data elements and would render most state actions impossible.
Louisiana	SB 449	STUDENTS: Provides relative to the privacy and protection of student data for students enrolled in public elementary, secondary, and postsecondary educational institutions.	This bill would require the State Board and the postsecondary education management boards to develop and implement student data privacy policies and procedures. The bill would require data element definitions, a public data inventory (including proposed data elements and elements collected for no reason), and a policy in alignment with FERPA (including role-based access rules, the creation of a CPO and their responsibilities, and rules for breach notification, security procedures, audits and	2/28/2014	Withdrawn	No	Yes	No	This bill describes governance and data privacy protections without being prohibitive. This bill adopts many of

			transparency of results, privacy standards, and contractor reviews). The bill would prohibit the disclosure of data across data lines with certain exceptions including working with a service provider or data management contractor.						the provisions outlined in OK HB 1989.
Maine	LD 1194	"An Act To Protect Social Media Privacy in School and the Workplace"	This bill would establish a Joint Standing Committee on Judiciary to, among other tasks, study student privacy especially with regard to social media and cloud computing services, concerns of parents about online education data service providers using data to build student profiles and for targeted online advertising, and how other states address student privacy with social media and cloud computing services. The committee will present findings and privacy recommendations (including legislative recommendations) to the	3/26/2014	Passed into law (veto overridden)	No	Yes	No	This bill would not direct any action beyond the convening of a committee to study student privacy in the context of social media and cloud

			legislature.						computing service providers.
Maine	LD 1780	An Act To Prohibit Providers of Cloud Computing Service to Elementary and Secondary Educational Institutions from Processing Student Data for Commercial Purposes	This bill would prohibit a cloud computing service provider that provides a cloud computing service to an educational institution from using that service to process student data for any secondary use that benefits the provider or any 3rd party.	2/13/2014	Died in Committee	Yes	No	No	This bill reiterates existing data sharing permissions and does not describe any governance efforts.

Maryland	HB 1508	Educational Agencies and Institutions – Education Records – Disclosure of Personally Identifiable Information	This bill would allow an educational agency or institution to designate a person as an authorized representative to conduct a specified audit, evaluation, or compliance or enforcement activity only if the person is under the direct control of the agency or institution. The bill would prohibit the disclosure of PII to a contractor, consultant, or other party without written consent except under specified conditions (including service delivery, legal duties, and student supports). The bill would also require that PII data are destroyed five years after the student's last enrollment in an in state educaiton institution. The bill would establish a public data inventory and require information on data management procedures, breach procedures and accountability, and penalties for the misuse of data.	2/27/2014	Introduced	Yes	Yes	No	This bill describes data governance measures and data privacy protections and seeks to increase transparency while limiting some data disclosures.

Maryland	HB 607	Student Privacy and Cloud Computing Act	This bill would allow educational institutions to work with cloud service providers and provide cloud computing to students and educators. The bill also reiterates some of the service provider usage limitations described in FERPA including that data cannot be sold, used for commercial purposes or other purposes that benefit the service provider.	1/30/2014	Passed in the House	Yes	Yes	No	This bill reiterates existing data sharing prohibitions and allows for the use of cloud computing services.
Maryland	SB 833	Educational Agencies and Institutions – Education Records – Disclosure of Personally Identifiable Information	This bill would limit the disclosure of PII (with exceptions for research, improving instruction, delivering services, etc.). The bill reiterates existing prohibitions on the selling of data or its use for commercial purposes. The bill would also provide for governance around data collection, breach notification, data retention and destruction, and transparency/public notification.	1/31/2014	Introduced	Yes	Yes	No	This bill reiterates existing data sharing prohibitions while also providing comprehensive governance, transparency, and accountability measures.

Massachusetts	HB 331	An Act prohibiting service providers who offer cloud computing services to K-12 educational institutions from processing student data for commercial purposes	This bill would prohibit K-12 cloud computing service providers from using student data for commercial purposes.	1/15/2013	Introduced	Yes	No	No	This bill was introduced in 2013, but remains technically active. This bill reiterates existing limitations and does not describe any governance efforts.
Mississippi	SB 2632	Common Core National Education Standards and P.A.R.C.C.; prohibit State Board of Education from implementing.	This bill would prohibit the state from expending certain federal funds to track students beyond K-12 and to distribute certain student PII.	1/20/2014	Died in Committee	Yes	No	Yes	Defunding of the SLDS is in direct opposition to DQC data elements and would render most state actions

									impossible. Much of this bill deals with Common Core and the state's participation in PARCC.
Mississippi	SB 2737	State Longitudinal Data System (SLDS); prohibit SDE from implementing and repeal.	This bill would prevent the state school board, state DOE, or any district from expending funds on the implementaiton of an SLDS that tracks students beyond K-12 or for releasing any PII or education data to an outside entity. This bill would also repeal existing statute that authorizes the SLDS.	1/20/2014	Died in Committee	Yes	No	Yes	Defunding of the SLDS is in direct opposition to DQC data elements and would render most state actions impossible.

Mississippi	SB 2436	State Longitudinal Data System (SLDS); allow parents of public school students to opt-out of mandatory electronic tracking system.	This bill would require that the SLDS governing board allow parents of public school students to opt-out of the "mandatory electronic data educational tracking system."	1/20/2014	Died in Committee	Yes	No	Yes	Weakening the SLDS is in direct opposition to DQC data elements and would render most state actions impossible.
Mississippi	SB 2736	An Act to provide that the state board of education and the state department of education shall take no further action to implement any Common Core Standards...; To repeal sections 37-154-1 and 37-154-3, Mississippi Code of 1972, which provide for the devel	This bill would halt the state implementation of the Common Core State Standards and would require the state to create its own curriculum content advisory committee. The bill would also prohibit the MS DOE from using any federal SLDS funds and would repeal the state law enacting the SLDS.	1/20/2014	Died in Committee	Yes	No	Yes	Defunding of the SLDS is in direct opposition to DQC data elements and would render most state actions impossible.

Mississippi	SB 2752	AN ACT RELATING TO STUDENT RECORDS; CREATING THE "MISSISSIPPI STUDENT DATA ACCESSIBILITY, TRANSPARENCY AND ACCOUNTABILITY ACT OF 2014"	This bill would charge the school board with producing a public data inventory of collected and proposed PII and to develop policies to outline data access (which allows access by service providers) and security. The bill would prohibit the transfer of some data; the bill would prohibit the release of PII for research purposes.	1/20/2014	Died in Committee	Yes	Yes	No	The bill seeks to govern data use and ensure student privacy, but prohibits some disclosures. This bill adopts many of the provisions outlined in OK HB 1989.

Missouri	SB 815	AN ACT To repeal section 160.514, RSMo, and to enact in lieu thereof four new sections relating to the duties of the state board of education	This bill would charge the school board with promulgating a rule related to SLDS student data accessibility, transparency, and governance. The rule will include a mandate for the SEA to produce a public inventory of collected data elements and proposed data elements. The rule would also specify who has access to PII in the SLDS (including service providers) and provide for the development of privacy and security policies (including audits, data destruction, and breach responses). The rule would also ensure that contracts with data management providers are enforced to protect privacy. The bill also prohibits the collection of limited data (juvenile court records, criminal records, biometric data, political affiliations, religion). [Note: While not companion bills, HB 1157 and HB 1490 include the same data privacy language]	2/3/2014	Introduced	Yes	Yes	No	The bill seeks to govern data use and ensure student privacy without being very prohibitive (very limited data collection is prohibited). Much of this bill deals with the selection of state performance standards and the state's participation in

	assessment consortia. This bill adopts many of the provisions outlined in OK HB 1989.

Missouri	HB 1157	AN ACT To amend chapter 161, RSMo, by adding thereto one new section relating to the privacy of student data.	This bill would charge the school board with promulgating a rule related to SLDS student data accessibility, transparency, and governance. The rule will include a mandate for the SEA to produce a public inventory of collected data elements and proposed data elements. The rule would also specify who has access to PII in the SLDS (including service providers) and provide for the development of privacy and security policies (including audits, data destruction, and breach responses). The rule would also ensure that contracts with data management providers are enforced to protect privacy. The bill also prohibits the collection of limited data (juvenile court records, criminal records, biometric data, political affiliations, religion). [Note: While not companion bills, SB 815 and HB 1490 include the same data privacy language]	1/8/2014	Passed in the House	Yes	Yes	No	The bill seeks to govern data use and ensure student privacy without being very prohibitive (very limited data collection is prohibited). This bill adopts many of the provisions outlined in OK HB 1989.

Missouri	HB 1490	AN ACT To repeal sections 160.514, 160.518, 160.526, 160.820, and 161.092, RSMo, and to enact in lieu thereof eight new sections relating to elementary and secondary education standards, with an emergency clause.	This bill would charge the school board with promulgating a rule related to SLDS student data accessibility, transparency, and governance. The rule will include a mandate for the SEA to produce a public inventory of collected data elements and proposed data elements. The rule would also specify who has access to PII in the SLDS (including service providers) and provide for the development of privacy and security policies (including audits, data destruction, and breach responses). The rule would also ensure that contracts with data management providers are enforced to protect privacy. The bill also prohibits the collection of limited data (juvenile court records, criminal records, biometric data, political affiliations, religion). [Note: While not companion bills, SB 815 and HB 1157 include the same data privacy language]	1/16/2014	Passed in the Senate and House	Yes	Yes	No	The bill seeks to govern data use and ensure student privacy without being very prohibitive. Much of this bill deals with the selection of state performance standards and the state's participation in assessment consortia. A Senate substitute

	of the bill passed in the Senate and has been sent to the House. This bill adopts many of the provisions outlined in OK HB 1989.

Missouri	HB 1873	Establishes the Missouri Student Data Protection Act	This bill would prohibit the collection of biometric, religious, or other non-cogntive data without consent. The bill would prohibit predictive analyses without consent. The bill lists the data elements that may be collected (contact information, courses and greade, degree attainment, enrollment status, remediation, attendance, demographics, etc.). The bill would prohibit the use of funds to construct, enhance, or expand data systems to track students beyong K-12 beyond what is needed for either administrative functions directly related to a student's education or evaluation of academic programs and student progress.	2/13/2014	Introduced	Yes	No	Yes	Weakening the SLDS is in direct opposition to DQC data elements and would render most state actions impossible. This bill limits the maintenance and use of data without describing any governance measures.

Missouri	SB 819	Enacts multiple provisions to protect the privacy of individuals from government intrusion "Fourth Amendment Protection Act."	This bill would limit the student data that could be collected without parental consent to directory information, demographics, academic information, and some additional and extracurricular data. Other types of data can be collected with consent; no federal funds could be used to collect these data. The bill would require a public list of collected data elements and their authorization, protection, and purpose. The bill also provides for a contact person, audits, breach reporting, notification of rights. The bill would prohibit the use of assessments collecting psychological data or information on religion, mental health, sexual behaviors, illegal behavior, gun-ownership, etc. Access to student data would be restricted to those who need it for educational purposes. The bill would call for procedures for research and public requests. The bill reiterates prohibitions on service providers (and cloud providers) using data for purposes outside of their contracts. The bill would limit some data sharing and would prohibit predictive modeling for	2/3/2014	Introduced	Yes	Yes	Yes	Preventing certain data activities (e.g., predictive modeling) is direct opposition to DQC data elements and would render many state actions impossible. The bill limits the collection and use of data and also provides transparency and accountability measures

			any outcomes.						.
Missouri	HB 1250	AN ACT To repeal section 160.518, RSMo, and to enact in lieu there of two new sections relating to student assessment.	This bill would prohibit the collection of additional student data during the assessment process next year (as compared to the 2013-2014 year).	1/9/2014	Passed in the House	Yes	No	No	This bill could limit the collection of appropriate data during the assessment

									process. Much of this bill pertains to state assessment decisions.
New Hampshire	HB 312	Restricting the collection of biometric data by state agencies, municipalities, and political subdivisions	This bill restricts the collection of biometric data by state and local government agencies and provides a private right of action for the misuse or unlawful collection of biometric data.	1/3/2013	Passed in the Senate and House	Yes	No	No	This bill restricts the collection of biometric data by state and local agencies and does not describe any governance efforts.
New Hampshire	HB 1262	Relative to student assessment data privacy	This bill restricts the collection, storage, and sharing of student assessment data by the United States Department of Education and the New Hampshire department of education. The bill gives districts the authority to decide not to send PII out of the	1/8/2014	Introduced	Yes	No	Yes	This bill restricts the collection of biometric and other data by

			district. The bill also prevents the collection, storage, or sharing of biomentric, religious, political, health, criminal record data, or birthdates or SSN.						state agencies and does not describe any governance efforts.
New Hampshire	HB 1586	AN ACT relative to student and teacher information protection and privacy.	This bill establishes procedures for protecting the privacy of student and teacher PII. The bill also prohibits the use of video monitoring in a classroom for the purpose of teacher evaluations, or the use of many other observational methods without written parental consent.	1/8/2014	Introduced	Yes	Yes	Yes	This bill establishes privacy audits and related procedures, but also prohbits predictive analytics and the use of data for other legitimate education purposes, rendering most DQC state actions impossibl

									e.
New Hampshire	HB 1587	Relative to the collection and disclosure of pupil data.	Except as provided for in the state's data system statute, this bill would prohibit the state DOE from sharing any PII data with any public or private individual or entity (including the government and those involved in the pupil's education) for any reason.	1/8/2013	Signed into law	Yes	No	No	This bill takes a prohibitive approach, but does not apply to the activities of the state's data system which allows data sharing between state agencies and storage in data

									warehouses.
New Jersey	SB 2189	Concerning cloud computing service provider contracts with public, private, or charter schools and supplementing Title 18A of the New Jersey Statutes.	This bill would prohibit contracted cloud computing service providers from disclosing data collected from public, private, or charter schools except to a student, teacher, or staff member of the school. The bill would require the cloud service provider to "process or monitor" an educational record only as needed to provide their contracted service and that this be in writing.	6/16/2014	Introduced	Yes	No	No	This bill reiterates existing prohibitions on service providers.
New Jersey	AB 3147	AN ACT concerning cloud computing service provider contracts with public, private, or charter schools and supplementing Title 18A of the New Jersey Statutes.	This bill would prohibit cloud computing service providers from disclosing data collected from schools (public, private, or charter) to any person other than a student, teacher, or staff member of the school. The bill would require cloud computing service providers to monitor the integrity of their systems. The bill would establish civil penalties for the misuse of data.	5/15/2014	Introduced	No	No	No	The bill reiterates existing prohibitions on the diclosure of data by service providers without describing any

									governance measures.
New Jersey	AB 3081	AN ACT concerning education reform and initiatives, and supplementing P.L.2012, c.26 (C.18A:6-117 et al.) and chapter 7C of Title 18A of the New Jersey Statutes.	This bill would establish an Education Reform Review Task Force responsible mainly for investigating CCSS and PARCC and other assessment options, but also for issues related to student data. With regards to PARCC, the task for would conduct an "evaluation of issues related to the use and data mining of student and family personal data and a student's right to privacy. The task force shall consider, but not be limited to, data related to learning disabilities, student behavior, political affiliation, religious affiliation, and medical history."	5/8/2014	Passed in the Assembly	No	No	No	Calls for an investigation of data use without being prohibitive or describing any data governance measures. Much of this bill deals with the selection of state performance standards

									and the state's participation in assessment consortia.
New York	AB 8556	A BUDGET BILL, submitted by the Governor pursuant to article seven of the Constitution	This bill would prohibit the state DOE from providing PII to service providers (and call for the destruction of any data already provided) and would allow districts to opt-out of providing student PII to any party for inclusion in a data dashboard. The bill would also require the implementation of a CPO with specific responsibilities including making security and privacy policy recommendations and developing procedures for transparency, notification and parent complaints. The bill also calls for a parents bill of rights, a data inventory, and lays out guidelines for contracting with service providers. [Note that this is the Assembly	1/21/2014	Signed into law	Yes	Yes	No	Prohibitions on sharing data with service providers could limit future education data work. This bill addresses student data privacy through the state's

			version of SB 6356 below]						budget.
New York	SB 6356	A BUDGET BILL, submitted by the Governor pursuant to article seven of the Constitution	This bill would prohibit the state DOE from providing PII to service providers (and call for the destruction of any data already provided) and would allow districts to opt-out of providing student PII to any party for inclusion in a data dashboard. The bill would also require the implementation of a CPO with specific responsibilities including making security and privacy policy recommendations and developing procedures for transparency, notification and parent complaints. The bill also calls for a parents bill of rights, a data inventory, and lays out guidelines for contracting with service providers.	1/21/2014	Signed into law	Yes	Yes	No	Prohibitions on sharing data with service providers could limit future education data work. This bill addresses student data privacy through the

			[Note that this is the Senate version of AB 8556 above]						state's budget.
New York	AB 8929	AN ACT to amend the education law, in relation to reforms in common core	This bill would delay the use of state or local assessments (including assessments aligned to the CCSS) for several purposes including teacher and principal evaluation, and inclusion in students' records. The bill would allow parents to opt-out of having their child's PII or biometric data shared with any third party; the bill would require the DOE to produce a list of third parties parents can opt-out from. The bill would prohibit districts from sharing PII with service providers unless certain security provisions are met in writing. The bill would require CCSS related PD and tools for teachers.	2/28/2014	Introduced	Yes	No	Yes	Opt-out compromises the state data system and renders most DQC state actions impossible. This bill restricts the use of data for education purposes and does

									not describe any governance efforts.
New York	AB 7243	AN ACT to amend the education law, in relation to enacting the "K12 student privacy and cloud computing act"	This bill would prohibit service providers who offer cloud computing services to primary and secondary educational services from processing student date for commercial purposes. Any service provider must comply with these terms in writing. [Note: This is the Assembly version of SB 5355 below]	5/8/2013	Introduced	Yes	No	No	This bill was introduced in 2013, but remains technically active.
New York	SB 5355	AN ACT to amend the education law, in relation to enacting the "K12 student privacy and cloud computing act"	This bill would prohibit service providers who offer cloud computing services to primary and secondary educational services from processing student date for commercial purposes. Any service provider must comply with these terms in writing. [Note: This is the Senate version of AB 7243 above]	5/16/2013	Introduced	Yes	No	No	This bill was introduced in 2013, but remains technically active.

New York	SB 6007	AN ACT to amend the education law and the penal law, in relation to establishing penalties for the unauthorized release of personally identifiable information from student records and certain records of classroom teachers and building principa	This bill calls for the development of data privacy and security standards, creates processes for increased data transparency, and establishes penalties for the unauthorized release of PII from student records and certain records of classroom teachers and building principals. [Note: This is the Senate version of Assembly Bill 8353 below]	12/11/2013	Introduced	No	Yes	No	While not perfect, this bill lays out ciritcal governance guidelines without restricting appropriate data use.
New York	AB 8353	AN ACT to amend the education law and the penal law, in relation to establishing penalties for the unauthorized release of personally identifiable information f	This bill calls for the development of data privacy and security standards, creates processes for increased data transparency, and establishes penalties for the unauthorized release of PII from student record and certain records of classroom teachers and building principals. [Note: This is the Assembly version of Senate Bill 6007 above]	1/9/2014	Introduced	No	Yes	No	While not perfect, this bill lays out ciritcal governance guidelines without restricting appropriate data use.

New York	SB 4284	AN ACT to amend the education law, in relation to the release of personally identifiable student information	This bill prohibits the release of personally identifiable student information where parental consent is not provided.	1/8/2014	Introduced	Yes	No	Yes	Limiting the use of PII data for legitimate education uses renders most DQC state actions impossible.
New York	SB 5932	An act to amend the education law, in relation to the release of personally identifiable student information	This bill would prohibit the release of PII to certain third parties without parental consent (unless required by statute, court order). Provides for a plan for data privacy and security protections including an annual data audit and remediation plan, and breach remediation procedures and transparency. The bill also calls for the creation of a publicly available list of the PII data collected and the authority under which it is collected. The bill would prohibit the commercial use of data and would prohibit the state DOE or board from maintaining PII data without consent unless its for legal, administrative, some research purposes, and the	9/11/2013	Introduced	Yes	Yes	No	This bill was introduced in 2013, but remains technically active. The bill prohibits some data sharing practices and also provides for governance and

			performance of job duties. [Note: This is the Senate version of AB 6059 below]						transparency of the PII that is collected and shared.
New York	AB 6059	Relates to the release of personally identifiable student information	This bill would prohibit the release of PII to certain third parties without parental consent (unless required by statute, court order). Provides for a plan for data privacy and security protections including an annual data audit and remediation plan, and breach remediation procedures and transparency. The bill also calls for the creation of a publicly available list of the PII data collected and the authority under which it is collected. The bill would prohibit the commercial use of data and would prohibit the state DOE or board from maintaining PII data without consent unless its for legal, administrative, some	3/13/2013	Passed By Assembly, Died in Senate, Returned to Assembly	Yes	Yes	No	This bill was introduced in 2013, but remains technically active. The bill prohibits some data sharing practices and also provides for governan

			research purposes, and the performance of job duties. [Note: This is the Assembly version of SB 5932 above]						ce and transparency of the PII that is collected and shared.
North Carolina	SB 815	AN ACT to ensure the privacy and security of student educational records	This bill would charge the state board with creating a public data inventory and corresponding data dictionary for all state and federal PII data mandates and data elements that are proposed for collection. The bill also charges the board with developing privacy and security policies in accordance with FERPA and other state laws to address data access, research requests, security audits and breach responses, and data rentention and destruction procedures. The bill would require that service providers adhere to privacy and security standards. The bill would require transparency about existing	5/20/2014	Signed into law	Yes	Yes	No	The bill describes data governance and transparency measures while limiting the inclusion of some data in student records.

			parental-opt out rights and would prohibit the inclusion of biometric, religious, and political data in a student record or SLDS.						
North Carolina	SB 806	Education Longitudinal Data System Changes.	This bill specifies that workforce data and data in the SLDS are individual student data. The bill would make the Board independent of any state agency and would give this body the responsibility to provide oversight on the SLDS and its users, to enter into contracts and ensure that contracts with service providers account for data privacy and security. [Note: This is the Senate version of HB 1150 below]	5/19/2014	Introduced	No	Yes	No	This bill begins to describe a new, more independent data governance body; the exact implementation of this work is not yet clear.

North Carolina	HB 1150	Education Longitudinal Data System Changes.	This bill specifies that workforce data and data in the SLDS are individual student data. The bill would make the Board independent of any state agency and would give this body the responsibility to provide oversight on the SLDS and its users, to enter into contracts and ensure that contracts with service providers account for data privacy and security. [Note: This is the House version of SB 806 above]	5/20/2014	Introduced	No	Yes	No	This bill begins to describe a new, more independent data governance body; the exact implementation of this work is not yet clear.
Ohio	HB 181	To prohibit submission of a student's personal identifiable information to the federal government without direct authorization of the local school board.	This bill prohibits the submission of a student's personal identifiable information to the federal government without direct authorization of the local school board.	5/29/2013	Passed in the House	Yes	No	No	This bill reiterates existing prohibitons and does not describe any governance efforts.

Ohio	HB 487	With regard to education provisions for students in grades kindergarten through twelve.	This bill would charge the state board of education with creating data confidentiality standards for student PII. The bill would also limit assessment data collected to data for measuring and improving the academic progress and needs of students, educators, school districts, and schools. The bill would also prohibit the collection of social security numbers, religion, political party affiliation, voting history, or biometric data as part of testing; this data also cannot be shared with any other entity including the federal or state government.	3/19/2014	Signed into law	Yes	Yes	No	This bill has some governance measures and reiterates some existing prohibitions. The privacy provisions are part of a very large bill on a number of broadly education-related topics including the state's adoption of CCSS and related assessments.

Oklahoma	HB 2911	An Act relating to schools	This bill would deauthorize other OK agency staff from accessing student PII, prohibit the linking of early childhood PII with K-12, PS, or workforce data, prohibit the linking of K-12 PII with PS or workforce data, prohibit the linking of any early childhood or K-12 PII with any data outside the DOE. The bill would also prohibit the storing of student data by any entity "independent of the State Department of Education" and prevent student data being collected through digital software or an app that could be shared with a third party. The bill would also require annual parental consent for any data disclosure not required by law. The bill would prohibit the funding of the SLDS. Finally, the bill would require the state to withdraw from any consortia or other agreement that would cede content or standards control.	2/3/2014	Passed in the House	Yes	No	Yes	Prohibiting the linking of data for educational purposes and defunding the SLDS are in direct to DQC data elements and would render most state actions impossible. This bill proposes alterations to the Student Data Accessibility, Transparency and

									Accountability Act of 2013 (created last year from OK HB 1989).
Rhode Island	HB 7124	AN ACT RELATING TO EDUCATION AND LABOR - SOCIAL MEDIA PRIVACY (would establish a social media privacy policy for students and employees)	This bill would prohibit schools or districts from presuring a student to disclose their social media passwords or divulge any social media activity. The bill also provides definitions related to cloud computing and would require all cloud service providers to use student data for their contracted purpose only and to certify this in writing. [Note: This is similar to SB 2095 below]	1/16/2014	Signed into law	Yes	No	No	This bill applies to social media privacy only.

Rhode Island	SB 2095	AN ACT RELATING TO EDUCATION - SOCIAL MEDIA PRIVACY	This bill would prohibit schools or districts from presuring a student to disclose their social media passwords or divulge any social media activity. The bill also provides definitions related to cloud computing and would require all cloud service providers to use student data for their contracted purpose only and to certify this in writing. [Note: This is similar to HB 7124 above]	1/23/2014	Signed into law	Yes	No	No	This bill applies to social media privacy only.
Rhode Island	HB 7095	RELATING TO EDUCATION - PAUL W. CROWLEY STUDENT INVESTMENT INITIATIVE	This bill would charge a commission investigating the possible adoption of the Common Core State Standards with evaluating the issue of student and family personal data. Specifically, the comission would study data mining and student privacy and would focus on data relating to learning disabilities, student behavior, political affiliation religious affiliation and medical history. [Note: This is the House version of SB 2135 below]	1/15/2014	Introduced	No	Yes	No	The bill seeks to govern data use and ensure student privacy. Much of this bill is about establishing a committee to consider CCSS adoption.

Rhode Island	SB 2135	RELATING TO EDUCATION - PAUL W. CROWLEY STUDENT INVESTMENT INITIATIVE	This bill would charge a commission investigating the possible adoption of the Common Core State Standards with evaluating the issue of student and family personal data. Specifically, the comission would study data mining and student privacy and would focus on data relating to learning disabilities, student behavior, political affiliation religious affiliation and medical history. [Note: This is the Senate version of HB 7095 above]	1/29/2014	Introduced	No	Yes	No	The bill seeks to govern data use and ensure student privacy. Much of this bill is about establishing a committee to consider CCSS adoption.
Rhode Island	HB 8052	AN ACT RELATING TO EDUCATION - STUDENT DATA-CLOUD COMPUTING	This bill would prohibit the use of data for commercial purposes by contracted cloud computing service providers.	4/10/2014	Introduced	Yes	No	No	This bill reiterates existing prohibitions without describing any governance measures.

South Carolina	SB 300	General provisions concerning education	This bill would prohibit the sharing of student level information with any third party without a joint resolution of the general assembly.	1/29/2014	Introduced	Yes	No	No	This bill could limit the use of third parties for the appropriate educational use of data. Much of this bill pertains to the adoption of state content standards and testing procedures.

South Carolina	HB 3893	A BILL TO AMEND SECTION 59-18-320, AS AMENDED, CODE OF LAWS OF SOUTH CAROLINA, 1976, RELATING TO THE ADOPTION OF NEW STATEWIDE EDUCATION STANDARDS AND ASSESSMENTS, SO AS TO PROVIDE SUCH AN ADOPTION MUST NOT BE IMPLEMENTED UNTIL APPROVED BY THE GENERAL ASS 'South Carolina Department of Education Data Use and Governance Policy'.	This bill would prohibit the SEA from collecting PII beyond what is required under IDEA. The bill would require SEA data to be reported in accordance with EDFacts. The bill would require that state data be stored securely and that access rules be established. The bill provides for staff training and the implementation of a Data Governance Committee to make decisions about data disclosures. The bill would charge every district to create a data governance and use policy to be monitored by the state.	4/9/2014	Signed into law	No	Yes	No	The bill seeks to govern data use and ensure student privacy without being prohibitive. Much of this bill is about establishing state content standards.

South Dakota	SB 63	An Act to protect the privacy of the records of individual students.	This bill would state that the state's existing student record statute does not authorize the collection of information that is not necessary for funding calculations, student academic progress determinations, or reports required by law. The bill would also prohibit students from being surveyed without consent on topics like political and religious beliefs, sex behaviors and attitudes, and gun ownership. The bill also prohibits the submitting of PII to the US DOE. Finally, the bill says PII is not public and that the department must develop security measures for the data.	1/17/2014	Signed into law	Yes	No	No	This bill reiterates existing prohibitons and does not describe any governance efforts in detail.

Tennessee	HB 1549	AN ACT to amend Tennessee Code Annotated, Title 49, relative to educational standards.	This bill would require that the data collected from content standard assessments be used only to track the academic progress and needs of students. The bill would prohibit student PII or religious, political, biometric, or psychological data from being collected, tracked, housed with, reported to or shared with the federal government. The bill would also prohibit the collection of student data for commercial, political, or product development purposes. [Note: This is the House version of SB 1835 below]	1/22/2014	Signed into law	Yes	No	No	This bill limits the collection and use of data and does not describe any governance measures. Much of this bill is about state authority to adopt content standards.

Tennessee	SB 1835	AN ACT to amend Tennessee Code Annotated, Title 49, relative to educational standards.	This bill would require that the data collected from content standard assessments be used only to track the academic progress and needs of students. The bill would prohibit student PII or religious, political, biometric, or psychological data from being collected, tracked, housed with, reported to or shared with the federal government. The bill would also prohibit the collection of student data for commercial, political, or product development purposes. [Note: This is the Senate version of HB 1549 above]	1/22/2014	Signed into law	Yes	No	No	This bill limits the collection and use of data and does not describe any governance measures. Much of this bill is about state authority to adopt content standards.

Tennessee	SB 1470	AN ACT to amend Tennessee Code Annotated, Title 10, Chapter 7, Part 5 and Title 49, relative to data.	This bill regulates the collection and release of data by the department of education. The bill requires the development of a public data inventory and dictionary and to create a publicly available privacy policy that includes standards, audit procedures, retention and destruction requirements, and gives needed data access to appropriate parties including teachers , vendors, and for reporting requirements. [Note: This is the Senate version of HB 1882 below]	1/10/2014	Introduced	No	Yes	No	This bill provides for public transparency around data collection and privacy protections without restricting appropriate data use. This bill adopts many of the provisions outlined in OK HB 1989.

Tennessee	HB 1882	As introduced, enacts the "Data Accessibility, Transparency and Accountability Act", which regulates the collection and release of data by the department and state board of education. - Amends TCA Title 10, Chapter 7, Part 5 and Title 49.	This bill regulates the collection and release of data by the department of education. The bill requires the development of a public data inventory and dictionary and to create a publicly available privacy policy that includes standards, audit procedures, retention and destruction requirements, and gives needed data access to appropriate parties including teachers , vendors, and for reporting requirements. [Note: This is the House version of SB 1470 above]	1/14/2014	Introduced	No	Yes	No	This bill provides for public transparency around data collection and privacy protections without restricting appropriate data use. This bill adopts many of the provisions outlines in OK HB 1989.

Tennessee	HB 2057	AN ACT to amend Tennessee Code Annotated, Title 49, Chapter 1, relative to student records.	This bill would define directory information and prevent the disclosure of any PII to any party without written consent. [Note: This is the House version of SB 2182 below]	2/4/2014	Introduced	Yes	No	Yes	This bill limits the collection and use of data and does not describe any governance measures. Limiting the use of PII data for legitimate education uses renders most DQC state actions impossible.

Tennessee	SB 2182	AN ACT to amend Tennessee Code Annotated, Title 49, Chapter 1, relative to student records.	This bill would define directory information and prevent the disclosure of any PII to any party without written consent. [Note: This the Senate version of HB 2057 above]	1/29/2014	Introduced	Yes	No	Yes	This bill limits the collection and use of data and does not describe any governance measures. Limiting the use of PII data for legitimate education uses renders most DQC state actions impossible.

Utah	SB 49	PARENTAL PERMISSION TO RELEASE STUDENT INFORMATION	This bill outlines permissible data disclosures in accordance with FERPA (and allows for the use of service providers). Except as provided for in FERPA, PII cannot be released to an out of state SEA or another entity without consent. The bill would charge the school board with developing a rule to govern the disclosure of PII as outlined above.	2/3/2014	Introduced	Yes	Yes	No	This bill reiterates existing law and provides some additional governance steps while also prohibiting limited activies.
Utah	HB 169	Student Privacy Act	The bill would allow for parental authorization for the collection, sharing, or access of "optional" student data (i.e., discipline reports, remediation efforts, special education data, demographics, program participation). The bill would prohibit the collection of psychological information. The bill describes permissible data uses and disclosures and requires parents be informed of how data are used and safeguarded. The bill would charge the school board with creating a public data inventory, listing data collected without a purpose and proposed data collections, instituting a student privacy coordinator, and	3/13/2014	Introduced	Yes	Yes	Yes	The required authorization of certain types of data would limit the power of some DQC actions. This bill incorporates both prohibitive and governan

			developing a privacy/security policy including guidelines for service providers and breach notification procedures.						ce elements.
Virginia	HB 1114	A BILL to amend the Code of Virginia by adding in Article 5 of Chapter 14 of Title 22.1 a section numbered 22.1-289.01, relating to student data; cloud computing.	This bill requires cloud computing service providers to only process and monitor student data according to their contract and not for any other purpose that benefits the service provider or another third party. [Note: This is the House version of Senate Bill 599 below]	1/13/2014	Introduced	No	No	No	This bill addresses cloud contracting only and does not describe any broader data privacy governance efforts.

Virginia	SB 599	A BILL to amend the Code of Virginia by adding in Article 5 of Chapter 14 of Title 22.1 a section numbered 22.1-289.01, relating to student data; cloud computing.	This bill requires cloud computing service providers to only process and monitor student data according to their contract and not for any other purpose that benefits the service provider or another third party. [Note: This is the Senate version of House Bill 1114 above]	1/13/2014	Introduced	No	No	No	This bill addresses cloud contracting only and does not describe any broader data privacy governance efforts.
Virginia	SB 242	Higher education; students' personal information.	This bill would prohibit public institutions of higher education from selling, trading, releasing, or otherwise distributing students' personal information, including names, addresses, phone numbers, and social security numbers, to third-party vendors.	1/23/2014	Signed into law	Yes	No	No	This bill prohibits the selling of student information and does not describe any governance efforts in detail.

Washington	HB 2133	AN ACT Relating to maintaining privacy of student educational records	This bill would require a review of current data collection, management, and sharing procedures and agreements. The bill also establishes a regular review of these procedures and agreements should the state participate in the Smarter Balanced assessment consortium or any other multi-state assessment consortium.	1/10/2014	Introduced	No	Yes	No	This bill was rewritten after its introduction. The bill requires a data audit and describes some governance measures. Much of this bill is about conditions of participation in the Common Core assessment consortia.

West Virginia	HB 4390	Improving the education of West Virginia children by developing better education standards	This bill would prohibit the state from collecting student or teacher PII without consent, from spending federal funds on a system designed to track students beyond K-12 or from collecting non-cognitive data beyond what is needed for federal compliance, "administrative functions directly related to the student's education", or "evaluation of academic programs and student progress." The bill would also prevent PII data from being shared outside of the state (with exceptions for cloud service providers and other parties that will not use the data for commercial or other secondary uses).	2/3/2014	Introduced	Yes	No	Yes	Limiting the use of PII data for legitimate education uses renders most DQC state actions impossible. This bill limits data collection and does not describe any governance efforts. Much of the bill is about state authority to create an advisory

									council for adopting content standards.
West Virginia	HB 4279	Creating the Citizen Privacy and Internet Activity Act	This bill would prohibit the use of online activity data for any secondary purpose. Providers (of internet, websites, search engines, cloud computing, etc.) who sell data or transfer it illegally are guilty of a misdemeanor.	1/23/2014	Introduced	Yes	No	No	The bill prohibits the selling of online activities data but does not describe any governance measures.

West Virginia	SB 420	Relating to data sharing in P-20W Longitudinal Data System	The purpose of this bill is to add Workforce West Virginia and the West Virginia Supreme Court of Appeals to the existing entities that are to enter into a state data sharing compact; add workforce data to the data that is to be included in the P-20W Longitudinal Data System; and create a governing board of the P-20W Longitudinal Data System.	1/23/2014	Passed in the Senate	No	Yes	No	This bill seeks to govern data effectively without being prohibitive.
West Virginia	HB 4316	Creating the student data accessability, transparency and accountability act	This bill describes state, district and school responsibilities in creating and maintaining a student data inventory with definitions and provides for a data governance officer and describes their responsibilities. The bill also limits when data can be shared but includes provisions for educators, policymakers, families, researchers, public reporting, service providers, and those authorized by data sharing agreements. The bill also requires the development of data security and access policies and a Privacy Incident Response Program. The bill charges the State Board to adopt the rules needed to implement these activities.	1/24/2014	Signed into law	No	Yes	No	This bill describes roles and responsibilities in data protection efforts without restricting appropriate data use. This bill adopts many of the provisions outlined in OK HB 1989.

Wisconsin	AB 616	AN ACT to create 118.125 (8) of the statutes; relating to: prohibiting the collection of a pupil's biometric data and the use of any device to assess a pupil's physiological or emotional state	This bill prohibits a school board from collecting any biometric data from a pupil without the pupil's parent or guardian consent in writing.	1/10/2014	Introduced	Yes	No	No	This bill restricts the collection of biometric data and does not describe any governance efforts. Changes may be coming.
Wisconsin	AB 618	AN ACT to repeal 115.297 (4) (b) 5.; to renumber and amend 118.125 (2) (d); to amend 115.28 (12) (a) 3., 115.297 (4) (a), 115.297 (4) (b) (intro.), 115.30 (1), 115.30 (2), 118.125 (2) (a), 118.125 (2) (g) 2. and 120.18 (1) (s); and to create 115.28 (61),	This bill excludes contractors, consultants, volunteers, or any other person to whom a school board has outsourced school services or functions from the term "school district official". This bill provides that PII can be provided to a public or private research organization only with written consent. This bill also prohibits the DPI from collecting for the SIS any information that is not required to be submitted to DPI.	1/10/2014	Introduced	Yes	No	No	This bill limits data collection and does not describe any governance efforts.

Wyoming	HB 179	Privacy in education	This bill would require consent for the collection, storage, access or sharing of all student educational data or PII. No student education data or PII could be shared in any way without consent. Consent would be required annually. Data that are collected will be used for existing public reporting activities. The bill would also establish penalties for unauthorized data use.	2/13/2014	Introduced	Yes	No	Yes	Limiting the collection and use of all education data for legitimate education uses renders most DQC state actions impossible. This bill limits data collection and does not describe any governance efforts.

Wyoming	HB 97	AN ACT relating to education	This bill would establish state education data security policies and protocols and institute penalties for data misuse. The bill prohibits the collection of non-cognitive or psychological data. The bill would prohibit the construction of expansion of the SLDS. The bill prohibits the diclosure of data especially for commercial/marketing purposes, but there are exceptions for cloud storage from a contracted service provider. Data can not be shared out of the state for economic or workforce development planning.	2/10/2014	Introduced	Yes	No	Yes	Defunding of the SLDS is in direct opposition to DQC data elements and would render most state actions impossible. This bill limits data collection and does not describe any governance efforts. Much of the bill is about funding (halting

									the use ARRA funding) and CCSS (prohibiting participation in Smarter Balanced consortium).
Wyoming	SF 79	AN ACT relating to education	This bill would provide for comprehensive privacy and security processes (including audits, breach notification procedures, compliance standards, and related policies).	2/11/2014	Signed into law	No	Yes	No	This bill seeks to govern data effectively without being prohibitive.

Note: Rows in red indicates that the state's 2014 session has concluded.

References

Bidwell, A. (2014, January 23). Parents worry student data will be used for marketing, not education. *USNews*. Retrieved from http://www.usnews.com/news/articles/2014/01/23/parents-worry-student-data-will-be-used-for-marketing-not-education

Bidwell, A. (2014, February 4). Obama announces nearly $3 Billion in education technology commitments. *USNews*. Retrieved from http://www.usnews.com/news/articles/2014/02/04/obama-to-announce-nearly-3-billion-in-education-technology-commitments

President's Council of Advisors on Science and Technology (2014). *Report to the President: Big Data and Privacy: A Technological Perspective*. Retrieved from http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

Common Sense Media. (2014). *Student Privacy Survey*. Retrieved from https://www.commonsensemedia.org/sites/default/files/uploads/about_us/student_privacy_survey.pdf

Hensley-Clancy, M. (2013, December 13). U.S. schools' approach to student data threatens privacy: study. *Reuters*. Retrieved from http://www.reuters.com/article/2013/12/13/us-usa-education-privacy-idUSBRE9BC10320131213

Herold, B. (2014a, January 29). Data collection: Student privacy survey. *Education Week*. Retrieved from http://www.edweek.org/ew/index.html

Herold, B. (2014b, February 24). Education leaders tackle student data privacy issues at summit. *Education Week*. Retrieved from http://www.edweek.org/ew/index.html

Herold, B. (2014c, May, 19). Major school research and assessment provider suffers data breach. *Education Week.* Retrieved from http://www.edweek.org/ew/index.html

Gilbertson, A. (2014, January 22). Advocates want to limit uses of student data. *89.3 KPCC*. Retrieved from http://www.scpr.org/blogs/education/2014/01/22/15651/advocates-want-to-limi

Kamisar, B. (2014, January, 7). InBloom sputters as data privacy hits the spotlight. *Education Week.* Retrieved from http://www.edweek.org/ew/index.html

Lawrence, J. (2013, March 4). Student data collection efforts spur privacy concerns, *Education News*. Retrieved from http://www.educationnews.org/online-schools/student-data-collection-efforts-spur-privacy-concerns/

Leichty, R., Winnick, S., & Lipper, K. (2014). *Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy, and Security: Guidance for State Policymakers*. Retrieved from EducationCounsel, LLC website: http://www.educationcounsel.com/docudepot/articles/EducationCounsel%20Guidance%20on%20State%20Student%20Privacy%20and%20Security%20Policies%20-%204838-6763-1641%20v%201.pdf

Lu, A. (2013, December 17). Protecting student privacy in the data age, *The Huffington Post.* Retrieved from http://www.huffingtonpost.com/2013/12/17/student-data-privacy_n_4460582.html

Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology* (NIST Special Publication 800-145). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Molnar, M. (2014, April 16). Ed. industry groups outline steps to protect privacy of student data. *Education Week*. Retrieved from http://www.edweek.org/ew/index.html

Nagel, D. (2014, January 22). Concerns over student data privacy widespread among Americans. *The Journal*. Retrieved from http://thejournal.com/articles/2014/01/22/concerns-over-student-data-privacy-widespread-among-americans.aspx?m=2

National School Boards Association. (April 2014). *Data in the cloud: A legal and policy guide for school boards on student data privacy in the cloud computing era* (Report version 1.0). Retrieved from http://nsba.org/sites/default/files/reports/DataInTheCloud_Guide_NSBA_COSA.pdf

Osborne, C. (2014, January 23). Parents want transparency from schools concerning use of student data. *ZDNet*. Retrieved from http://www.zdnet.com/parents-want-transparency-from-schools-concerning-use-of-student-data-7000025493/

Plunkett, L., Solow-Niederman, A., & Gasser, U. (June 3, 2014). *Framing the law & policy picture: A snapshot of K-12 cloud-based Ed Tech, & student privacy in*

early 2014 (Research Publication No. 2014-10).Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2442432

Rice, A. (2014, April 28). Re: NSBA issues student data privacy guide in cloud computing era. [Newsgroup]. Retrieved from http://schoolboardnews.nsba.org/2014/04/nsba-issues-student-data-privacy-guide/

Reidenberg, J., Russell, N. C., Kovnot, J., Norton, T. B., Cloutier, R., & Alvarado, D., (2013). *Privacy and Cloud Computing in Public Schools. Center on Law and Information Policy* (Book 2). Retireved from http://ir.lawnet.fordham.edu/clip/2

Resmovits, J. (2014, January 22). Immense unease over advertisers nabbing student data: Poll, *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/2014/01/22/student-data-privacy-poll_n_4640688.html

Robinson, J. (2014, February 24). Sharing student data In the cloud: Should we be worried? *Northwest News Network*. Retrieved from http://hereandnow.wbur.org/2014/02/24/student-data-privacy

Sanchez, C., (2014, February 17). Survey: Students' personal data are at risk, *NPR*. Retrieved from http://www.npr.org/2014/02/17/278389264/survey-students-personal-data-are-at-risk

Schaffhauser, D. (2010, June 15). School districts stumble on data privacy, *The Journal*. Retrieved from http://thejournal.com/articles/2010/06/15/school-districts-stumble-on-data-privacy.aspx

Singer, N. (2013a, October 5). Deciding who sees students' data, *The New York Times*. Retrieved from http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html?pagewanted=all&_r=0

Singer, N. (2013b, October 13). Group presses for safeguards on the personal data of schoolchildren. *The New York Times.* Retrieved from http://www.nytimes.com/2013/10/14/technology/concerns-arise-over-privacy-of-schoolchildrens-data.html?ref=natashasinger&_r=0

Singer, N. (2014c, February 20). Scrutiny in California for software in schools. *The New York Times*. Retrieved from http://www.nytimes.com/2014/02/20/technology/scrutiny-in-california-for-software-in-schools.html?ref=technology&_r=1

Sheehy, K. (2014, January 13). Questions parents should ask about student data security. *USNews*. Retrieved from http://www.usnews.com/education/blogs/high-

school-notes/2014/01/13/4-questions-parents-should-ask-about-student-data-security

Strauss, V. (2014, March 6). Why a 'Student Privacy Bill of Rights' is desperately needed, *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed/

Svitek, P. & Anderson, N. (2014, February 19). U.Md. computer security attack exposes 300,000 records. *The Washington Post*, Retrieved from http://www.washingtonpost.com/local/college-park-shady-grove-campuses-affected-by-university-of-maryland-security-breach/2014/02/19/ce438108-99bd-11e3-80ac-63a8ba7f7942_story.html

Vacar, T. (2014, January 22). Group fights for student online privacy rights. *KTVU.* Retrieved from http://www.ktvu.com/news/news/education/group-fights-student-online-privacy-rights/ncyYs/