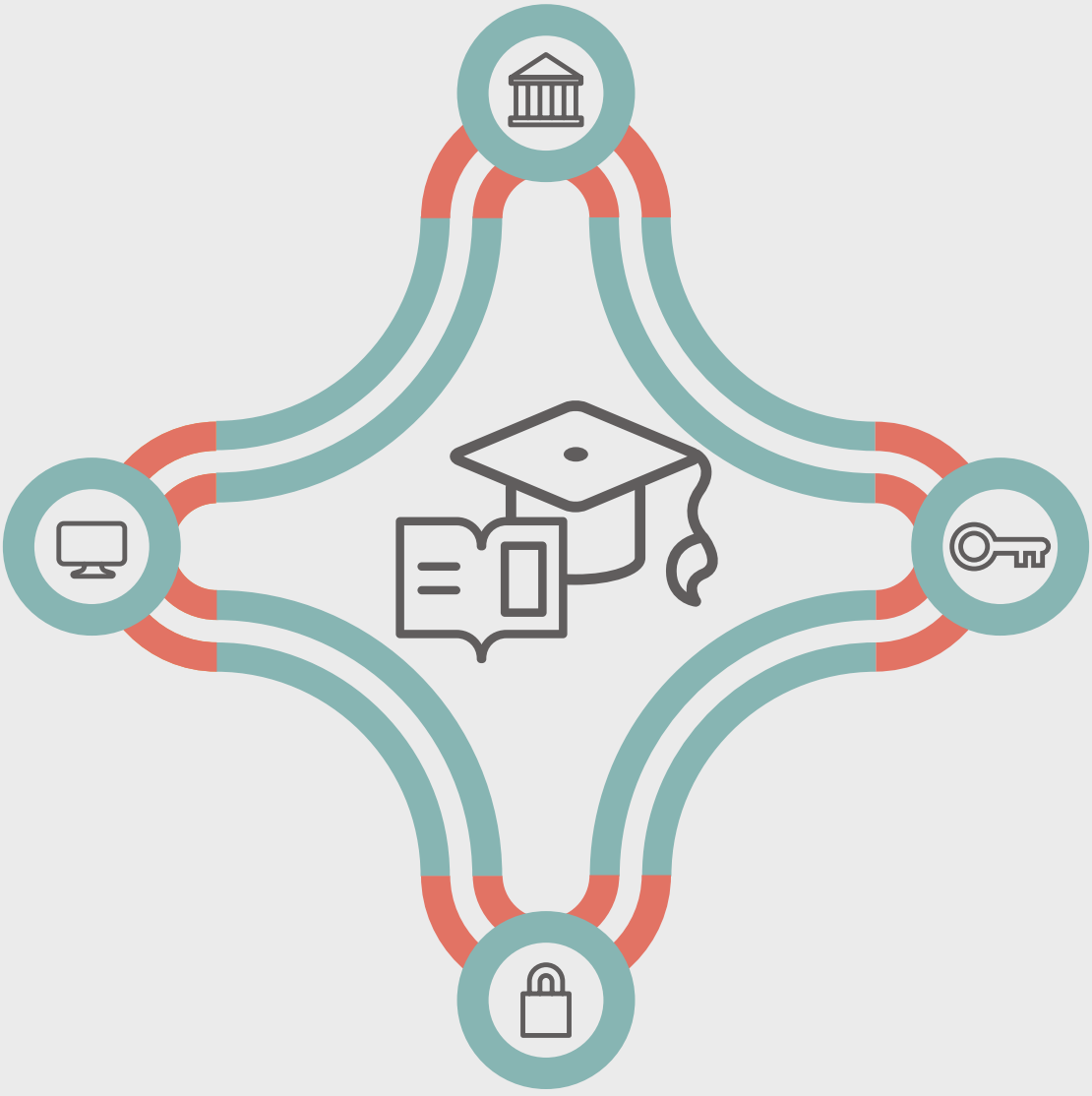
The Emergence of Data Privacy Conversations and State Responses

AUTHOR: RACHEL ANDERSON, DATA QUALITY CAMPAIGN

MAY 2019



Rachel Anderson is the Director, Policy and Practice at the Data Quality Campaign.

This paper is part of the larger series *Protecting Students, Advancing Data: A Series on Data Privacy and Security in Higher Education*. In August 2018, the Institute for Higher Education Policy (IHEP) first convened a Privacy and Security Advisory Board of privacy and security experts and higher education experts to explore some of the most pressing data privacy and security issues of the day. The resulting paper series serves as a resource for policymakers as they develop sound postsecondary data policy and centers privacy and security as a top priority. This report is based on research with support from Arnold Ventures. The findings and conclusions contained within are solely those of the author.

SECURELY LINKED DATA SUPPORTS STUDENT SUCCESS

Data powers learning. And while local school districts and postsecondary systems each get value from the data they collect about their own performance, data's real power to answer important questions and illuminate what works happens when states securely connect student-level data from across these pieces of the pipeline and gets that longitudinal information into the hands of families, students, communities, and school and institutional leaders.

Secure state longitudinal data systems (SLDSs), from K-12 to postsecondary and into the workforce, empower educators to support their individual students, allow schools and districts to assess and improve how their schools prepare students for college and career, help postsecondary institutions and systems to understand where their students are coming from and how they move through school and into the workforce, and uncover inequities throughout the education pipeline. By securely linking data from K-12 and postsecondary systems, states are able to answer questions like:

- Are our K-12 schools preparing all students to succeed in different types of postsecondary programs?
- What supports and experiences in high school are associated with students succeeding in postsecondary programs?
- Which postsecondary institutions and programs are preparing students to find a good job after graduation?

SLDSs also support many of the administrative functions central to schools and districts.

Still, for educators, policymakers, and families to find value in data, they must be able to trust that students' privacy is protected and that their data is used in supportive, responsible, and transparent ways.

PROTECTING PRIVACY IS A CRITICAL COMPONENT OF DATA USE

For as long as education institutions, districts, and states have used data to support teaching and learning, they have developed privacy practices, data governance structures, and security measures. In addition, several federal laws govern the collection and access of student data.[1] Most notably, the Family Educational Rights and Privacy Act (FERPA) is the foundational federal law on the privacy of students' educational records. FERPA safeguards student privacy by limiting who may access student records, specifying for what purpose they may access those records, and detailing what rules they must follow when accessing the data.

While data privacy and security have always been part of states' education work, for many years these topics were widely viewed as compliance issues or the sole purview of IT professionals; education data privacy was rarely a focus of state legislation. That changed abruptly in 2014 as public questions and concerns about how education data is used and protected mobilized state legislators to respond.

This shift in legislator focus was precipitated by growing concern both about the appropriate use of education data as well as privacy concerns related to data collection and use in almost every area of public life, from the National Security Agency to companies like Target to financial institutions to health care. This growing discourse about data provided an opportunity for conversations about the value of education data. It also created a context in which many state policymakers and education leaders felt they needed to take action in response to either an immediate and specific situation (e.g., contracting with data management services or implementing new statewide assessments) or more general concerns about government overreach, the implications of collecting information about individuals, and the activities of online data service providers.

Questions about how data is used to support learning ,and the legitimate need to clarify and modernize state policies about how data is used and protected, resulted in state policymakers taking action to safeguard student data privacy through communications, executive orders, and especially through state legislation.

STATE LEGISLATORS TAKE ACTION

In 2014, state legislators turned the privacy conversation into legislative action.[2] That year, 36 states introduced 110 bills addressing education data privacy and 20 states passed 28 of these bills into law. While these 110 bills represented diverse approaches to safeguarding privacy, most sought to answer the same basic questions:

- What are SLDSs, and how does data remain safeguarded while moving through them?
- What are the appropriate uses of data in supporting students and improving districts and institutions?
- How do the data management service providers that states, districts, and institutions use function and safeguard data?

To answer these questions, state legislators looked to two general approaches:

- Prohibitive: This approach seeks to ensure student privacy by preventing or halting the collection of a certain type of data (e.g., biometric data) or a certain data use (e.g., predictive analytics). In 2014, 79 of the 110 education data privacy bills introduced employed this approach.
- Governance: This approach seeks to amend or establish the procedures (e.g., security audits, public lists of data collected), roles and responsibilities (e.g., establishment of a CPO, description of school board and legislature roles), and supports (e.g., state leadership) needed to ensure that data are used appropriately. In 2014, 52 of the 110 education data privacy bills introduced employed this approach.

These two approaches are not mutually exclusive and in many instances the same piece of legislation used both of these approaches. For example, the same bill may prohibit the state from collecting data on students' religious or political beliefs, and also establish new governance processes for how the state chooses and contracts with a data management provider.

While neither of these approaches is "correct," and many of the most robust privacy bills incorporate both approaches, aiming to protect privacy only by limiting data collection and use does nothing to safeguard the data that states are already collecting for accountability, legal, continuous improvement, and transparency purposes. Instead, policymakers are well-served by thinking proactively about creating effective and transparent data governance.

Louisiana's Efforts to Safeguard Education Data Privacy

SETTING THE STAGE: LOUISIANA IN 2014

In 2014, while conversations about the appropriate use, linking, and protection of education data were taking place across the nation, concerns and confusions were especially pronounced in Louisiana. This was due in part to the state's planned participation in inBloom, a data management service designed to securely house schools' and districts' data in order to connect different data sources and make the data more accessible and useful for educators and school leaders.[3]

Louisiana was one of nine states that had agreed to pilot the use of inBloom, but as the launch date neared, public pushback emerged. This came from a lack of publicized stakeholder engagement in the decision to use inBloom and a confusion about what inBloom was, who would have access to the data stored in it and for what purpose, and what the benefits would be for educators and students. What started as questions and concerns about inBloom quickly revealed a general lack of public understanding about the role of data in education and how schools, districts, and states collected and used data to support students and improve schools. Administrators recognized they had not done enough to educate the public about how data are used and the value these data

can provide in improving student success. Reflecting on a contentious 2013 Board of Elementary and Secondary Education meeting on inBloom's use, State superintendent John White acknowledged, "I heard the comments from parents who had concerns, and I said 'Look, this isn't something we have really talked about in public to a great extent.' I'm not talking just about inBloom, I'm talking about the entire question of how we store data and student info."[4]

Superintendent White announced that the state would withdraw from participating in inBloom (as did the other states and districts that had planned to pilot the service) in response to this lack of public understanding about how data was used at the state and district levels. At the same time, the public concern and confusion that had emerged were spurring conversations across the state and among lawmakers.

LOUISIANA'S STATUTORY BACKGROUND

Like in most states, when Louisiana lawmakers began looking to address student data privacy in 2014, the state had no existing statute that explicitly addressed education data privacy. However, existing state statutes did cover education data collection, the transfer of student records, and the collection of student biometric information.

Data Collection

In 1998, Louisiana enacted Revised Statutes 17:3911 (Data collection system; establishment), which created the SLDS. The statute outlined the types of data the state would include in its SLDS to contribute to state accountability, transparency, and decision-making:

- Results of assessments required by law or by board regulation;
- College readiness test information;
- School performance scores;
- Dropout rates;
- Student attendance rates;
- High school completion rates;
- Faculty information;
- Financial information;
- Student discipline information, including suspensions and expulsions;
- Class size information;
- Faculty attendance rates;
- Number of students in advanced placement classes and National Merit Scholarship finalists and semi-finalists;
- Socio-demographic student information; and
- Such other data as the board may approve.

The statute charged the Louisiana Department of Education with operationalizing these requirements by developing definitions for the data elements, creating reporting procedures for districts, and coordinating and managing education data collection activities across the state. This law did not explicitly articulate how education data privacy would be protected nor how any information may be appropriately shared. And while the statute included numerous data elements relevant to both K-12 and postsecondary stakeholders, the law did not explicitly address how these data elements could benefit institutions of higher education.

Transfer of Student Academic Records

Louisiana Revised Statute 17:112 (Student academic records; transfer; parental rights) was created in 2001 to govern the transfer of student academic records among state education entities. This law requires public elementary and secondary schools to transfer a student's education records to any new school where that student is enrolling or applying. (The law does not address the transfer of records to institutions of higher education.) The law requires a written request from an authorized person on behalf of the student's new school in order to transfer the records.

In addition, this law reiterates pieces of FERPA to state that parents and adult students have the right to review their own education records.

Student Biometric Information

Revised Statute 17:100.8 (Student biometric information; collection and use) was enacted in 2010. The law requires parent or adult student permission for the collection of biometric data (defined as "electronic measurement and evaluation of any physical characteristics that are attributable to a single person," such as a fingerprint or facial characteristics) and specifies that this data can only

be used for identification or fraud prevention purposes. The law also requires the governing authority of each public elementary and secondary school that collects biometric information to develop, adopt, and implement policies to secure the data and govern how and why it would be collected. The statute does not reference postsecondary institutions or systems.

LOUISIANA'S 2014 LEGISLATIVE RESPONSE

In response to national conversations, local conversations, and the state's existing statutes on education data, lawmakers acted in 2014 to pass two new education data privacy laws. Act 837 sought to safeguard privacy by, with some exceptions, prohibiting districts from sharing identifiable student data with any entity outside the district without written consent. This law enacted some valuable data governance provisions, but it also represented a stark departure from how the state had previously managed and shared data and caused immediate disruptions in school functioning and state administration. The second law, Act 677, required districts to publicly post information about the data management services they used, what data was shared with them, and for what purposes. While this law established important transparency measures, it also led to unintended consequences that actually threatened student privacy.

Louisiana Act 837[5]

Along with other provisions related to the collection, use, and privacy of education data, this law:

- Prohibited schools and districts from sending personally identifiable information about students to any private or public entity, including the Louisiana State Department of Education.
- Described penalties for people who willfully violate the law which include fines of up to $10,000 and the possibility of three years in jail. Those who violated the law under any conditions could also be fined up to $10,000 and serve up to six months in jail.
- Required the state to develop a new system of unique student identification numbers that districts would assign to their students; previously the state had used students' social security numbers as identifiers within the state data system.

Under the new law, schools and districts were allowed to send aggregated or de-identified data to the state for administrative and auditing purposes. Individual student data could be securely shared with a public entity like the State Department of Education only with written parent permission.

To facilitate this significant change, whereby the state could no longer administer a student-level longitudinal data system, the law also required the state to create a new data system using unique student identification numbers. Districts would administer their own local data systems, although the law did permit them to contract with some data service providers (a common practice) and for service providers to access local data systems in ways commensurate with their contracted responsibilities.

The law also provided certain governance provisions including:

- With parental permission, allowing school districts to collect information on students, including transcript data, in order to send it to Louisiana postsecondary institutions and the Louisiana Office of Student Financial Aid (LOSFA) for application purposes.
- Requiring service providers contracting with districts to establish policies related to data access, privacy, breach notification and remediation, and privacy and security audits.
- Data destruction requirements.
- Reiterating parent and student permissions to access their own records.
- Prohibiting the sharing of student data for any commercial purposes except as described in a signed contract.
- Requiring parental permission forms to include more information on exactly what data is being collected and how it is being used.

In design, Louisiana's Act 837 adopted both prohibitive and governance-focused provisions. The widespread prohibitions on sending identifiable student data outside of the district's system without parental permission

slowed and complicated key activities at the local and state level. But other components of the law established strong data governance to articulate how decisions about data use would be made, how service providers and districts would be accountable for data privacy, and how the public would be made aware of how education data was used and shared.

Louisiana Act 677[6]

Moving concurrently through the Louisiana state house was the bill that became Act 677. This law focused on increasing transparency around how districts and the state department of education work with service providers and share education data.

Act 677 required districts and the state department of education to post on their websites within ten business days of executing a contract:

- A profile of every entity authorized to receive student data,
- A copy of the signed agreement between the department and the data recipient,
- A complete list of all the data elements being transferred,
- A statement about the intended use of the information,
- Contact information for a primary point of contact for people with questions about the data sharing agreement, and
- A process for parents to register a complaint related to a potentially unauthorized data transfer.

Responding to concerns that data was moving and being shared in opaque ways, these requirements were designed to provide a technical listing of all the entities and partners who received data as part of their work with districts; plus they sought to provide more narrative information on the goals and approaches of the state and districts' data use.

ACT 837: IMPLEMENTATION AND IMPACT

In many ways, Louisiana's 2014 education privacy laws reflected a serious and well-intended effort to consider the appropriate role of data in education, to hold districts and the state accountable for the ways they use and protect data, and to limit potentially unnecessary data sharing.

However, reports of disruptions in school functioning and confusion about how the law's provisions could be reported quickly emerged after the law's passing. Rapides Parish School Board counsel James Downs told the Board's Education Committee, "I don't see, frankly, how schools are going to function without the general release of information. It's impossible actually."[7]

State Superintendent White concurred saying, "This is going to be a system where the state essentially purges its databases of most everything that is used today to identify a kid. It's a wholesale change … in how the state's data systems inter-operate with the local school data systems and how the local school systems operate."[8]

> "I DON'T SEE, FRANKLY, HOW SCHOOLS ARE GOING TO FUNCTION WITHOUT THE GENERAL RELEASE OF INFORMATION. IT'S IMPOSSIBLE ACTUALLY.

Under the new law, districts were unable to automatically send student transcripts to Louisiana postsecondary institutions and the state financial aid office, complicating students' efforts to apply to those schools. It became more difficult for the state to provide data tools to educators, since the state couldn't have (and therefore report on) individual students' performance and progress. Further, the State Department of Education had to work with the Board of Regents to create a new consent form and process to transfer records and administer state scholarships.

The confusion and burdens of implementation fell largely to districts to navigate,[9] and, as a systems analyst from Bossier Parish Schools explained, many district-level staff were unaware of the bill's development and the sudden changes it would bring until it was already signed into law and the state department of education had formed a team to enact the new provisions. Local newspapers anticipated that the law might be interpreted to prohibit a school from listing valedictorians, athletes, or student guests at school board meetings and concluded that the "laws intended to protect student's private information are expected to have unintended consequences as drastic as criminal penalties for school districts."[10] Some districts who were suddenly charged with taking on more complex data management and use activities, which had previously been handled at the state level, worried that they lacked the capacity and expertise to confidently meet these new responsibilities.[11]

Many of the law's impacts were likely felt most acutely by the state's most vulnerable students and those who serve them. The Louisiana Department of Education relied on its statewide data system to identify and contact students eligible for a college scholarship program; the new law ended the state's ability to seamlessly provide this critical opportunity to students. Limiting the use of data for research, as the Louisiana law did, can stunt efforts to see and address inequities. In a piece for the *New York Times*, education researcher Dr. Susan Dynarski explained that when states limit research, "We run the risk of turning out the lights, leaving us blind to the enormous inequities in our schools and ignorant of what is effective in correcting them."[12]

Other policy experts asserted that policies like Louisiana's could compromise personalized learning efforts.[13] Sheryl Abshire, the chief technology officer for Calcasieu Parish schools, told *Education Week* that the 2014 law prompted important conversations and practice updates, but fears of data misuse shouldn't compromise learning: "We must be responsible around data but also responsible around student learning," she said. "We shortchange students and our community if we step back and say, 'This is too complicated, so we're not going to do it.'"[14]

ACT 677: TRANSPARENCY AND SECURITY

While it didn't receive the same degree of attention as Act 837, Act 677 also created unintentional, harmful consequences. In a post on Facebook, Louisiana State Treasurer John Schroeder explained that by requiring districts to publicly post so many details about their contracts and data sharing agreement with service providers, the law inadvertently "presented a roadmap to hackers."[15]

> "... [THE LAW INADVERTENTLY] PRESENTED A ROADMAP TO HACKERS.

The Fair Information Practice Principles[16] and similar frameworks highlight transparency as an important component of ethical data use. Louisiana's Act 677 shows how defining a meaningful transparency that provides clarity, without inappropriately tasking people to be the sole monitor of their privacy, can be difficult. Louisiana's law not only compromised data security by giving potential bad actors detailed information about data systems and infrastructure that they did not have access to previously, but by listing data elements and posting legal agreements, the law seemed to equate having technical information about how data was being shared with being prepared to assess which service providers were trustworthy data stewards and which uses of data were appropriate.

The law did outline several other transparency measures, notably profiles of each entity with access to data, information about the intended use of the data, and a contact person and process for parents to ask questions and lodge concerns. These descriptions help articulate a district's vision for data use and working with service provides, and can meaningfully help parents and adult students understand, question, and engage with how data is used to support learning.

2015 UPDATES

By 2015, Louisiana state legislators could see the unintended consequences of their earlier efforts. A local newspaper reported, "State Rep. Lance Harris, R-Alexandria, said this clearly was not the intent of the bill, which was authored by Rep. John Schroeder Sr., R-Covington. '[This] was to protect student data from data mining and that kind of thing.'"[17]

Consequently, lawmakers revisited Acts 837 and 677 in their 2015 legislative session and worked to lessen the laws' unintended consequences. The state worked with state- and district-level stakeholders, including staff specializing in education data collection and use, to understand the laws' impact and how to address their challenges. Act 228[18] made several clarifications to Act 837, gave districts more time to establish their new student identification systems, and, most importantly, gave districts the power to create district-level policies that allowed for data sharing as the district saw fit. In his Facebook post, Treasurer John Schroeder wrote "The local school boards asked me to add language to clarify that the law was not intended to prevent the schools from posting art work in the hallways, [creating a] school newsletter, [calling] out names of students at assemblies, etc.[—]and to extend the time they have to complete the unique student ID transition."

Districts took this new flexibility and quickly established their own data policies.[19] Districts created lengthy local policies to articulate how they planned to interpret and implement the law and some district leaders met with other local agencies like the juvenile court system to figure out how to continue to work together within the strict confines of the law.[20] Rapides Parish School Board counsel James Downs worked to develop updated

policies and a parent consent form to grant permission for his district to send high school transcripts to postsecondary institutions outside of Louisiana when students applied there. Downs told the *News Star,* "If we draft a policy carefully and work on it, I believe we can cobble something to get us by until the Legislature can review this [statute]. It will get us through without disrupting the entire fabric of the public school experience. We'll do the best we can."

In addition to the changes to 2014's Act 837, the state also amended Act 677 to prevent potential bad actors from accessing sensitive details about district contracts. The amendments require that districts make information about what companies they contract with and what data they share available for parents to see in person through the school district, rather than on a publicly-available website.

Ultimately, the responses of state policymakers and district leaders in Louisiana to the 2014 legislation resulted in some very positive outcomes, including clearer policies and guidance for districts and institutions, a careful examination of the data the state needed to meet its responsibilities, and greater transparency about data use and governance. Some district staff reported that they ultimately received a good amount of guidance from the state along with an avenue to ask direct questions when needed. Other state policymakers can seek to incorporate careful thinking on these issues into their initial legislation, rather than requiring local leaders and educators to sort through these complex issues later to redress unintended consequences.

LEARNING FROM OTHER STATES

While state policymakers must—and do—continue to refine and update their privacy laws and policies, many states have already demonstrated what proactive, positive, educator-informed education data legislation can look like.

- In 2015, Georgia passed a comprehensive data use and privacy law to safeguard students' data without limiting parent and educator access to the information they need to improve student achievement. Created with input from state officials, the law governs data collection and use both by the state and by online service providers used in schools.[21]

- In 2010, Maryland established by law the Maryland Longitudinal Data System Center, a statewide data system and governance structure designed to provide timely, accurate data and analyses from across state education and workforce agencies. The data system can be used to improve the state's education system and guide decisionmakers at all levels.[22]

- In 2016, Utah passed a law tasking the state board with developing a student data privacy governance plan, establishing advisory groups to make recommendations and provide feedback on data policies and practices, and designating a state student data officer to work with the state board on data privacy issues.[23]

Together these laws highlight the importance of grounding data legislation in educator needs, bringing diverse experts and decisionmakers together to look holistically at how and why data is used in education, and providing clear policies and guidance to local education leaders. While policymakers should always be working to learn more about how data can be used and protected, these state examples provide a template of thoughtful and robust data policy.

CONSIDERATIONS FOR FUTURE EFFORTS

The experiences of Louisiana lawmakers in 2014 and 2015, and of other states who have considered education data privacy legislation in recent years, highlight just how many factors are at play in articulating the role of data in education.

Lawmakers at state and federal levels can carry forward lessons learned from efforts in Louisiana to their own efforts. Policymakers should consider these recommendations as they work to ensure that longitudinal, student-level education data systems are tools to empower educators and families, address inequities, and improve learning for all students.

1 *Frame data privacy holistically as a component of data use:*

- **Start with questions.** Start conversations about data collection, linking, and systems with questions. What do we want to know? What data do we need to answer those questions? How can we safeguard data without compromising our ability to support student learning and improve our K-12 and postsecondary schools? Questions and needs should inform the construction and linking of data systems, not the other way around.
- **Understand data use and privacy as connected rather than competing ideas.** Safeguarding privacy is a critical component of effective data use. When looking to legislate data privacy, policymakers should consider the context of data use and the benefits of data use alongside any associated risks.
- **Focus on building capacity for effective, secure data use rather than on punitive consequences.** Enforcement consequences for willful data misuse can play an important role in safeguarding data privacy and in building public trust that compromising a student's privacy will not be tolerated. Since most instances of unauthorized data disclosure or data misuse are caused by human error, not malicious intent, policymakers have a responsibility to provide the trainings, models, and other agency staff supports that give professionals the skills and knowledge to prevent data privacy incidents.

2 *Understand the legislative landscape and engage diverse stakeholders to understand needs and the likely impact of legislation:*

- **Build from the landscape of existing statutes and laws.** Numerous state and federal laws and statutes already govern the use and privacy of student data.[24] Additional legislation should build on these foundational protections and ensure the alignment of definitions, requirements, and enforcement efforts.
- **Talk to educators to understand their needs and the impact of possible legislation.** Educators, district leaders, and postsecondary institution leaders are often at the front line of using data and protecting privacy. Policymakers should actively seek input from these and other local stakeholders as they draft and revise legislation to ensure that any new law or practice addresses a real need, avoids provisions that would be unnecessarily or unintentionally disruptive to educational institutions, and provides the implementation guidance and support that educators and local leaders need.
- **Consider equity implications.** Data can be a powerful tool for identifying and addressing education inequities. Under the Every Student Succeeds Act, states are charged with disaggregating data to understand how the state is serving different student populations, and many states publicly report data on college access and success for low-income students and students of color. Many states use data to identify and address inequities and to provide services like scholarships to students most in need. Policymakers must look at how any legislation limiting the use or sharing of data within the state may impact other state efforts to understand and improve opportunities for traditionally underserved students.

3 *Provide clarity and support for implementation:*

- **Provide support and guidance for implementation.** Protecting privacy isn't achieved with the passing of a law. Implementation of a new law or policy is critical to its success. When crafting any new legislation, policymakers must focus on the support and technical assistance (such as trainings for educators and staff, model contracts, and policies) that allow the state, districts, and postsecondary institutions to implement the law with confidence and fidelity.
- **Incorporate best practices and resources.** Since 2014, education and privacy experts have produced numerous recommendations and resources to guide the effective use and protection of education data. Policymakers should pull from best practices in privacy[25], consent[26], data deidentification[27], contracting[28], data security[29], and other topics.
- **Reduce burdens for families, schools, and districts.** Since 2014, many new state education data privacy laws have passed along much of the implementation efforts to school boards, local education agencies, institutions, and even individual parents. Policymakers should ensure that privacy protection efforts aren't burdens to students and educators, but a responsibility commensurate with data use.

Policymakers do not need to choose between using data to improve education and learning and safeguarding students' privacy. With careful consideration of needs, benefits, risks, and tools, policymakers can work alongside educators and education leaders to develop robust privacy protections without compromising the power of data to be a tool of educational equity and excellence.

Endnotes

1 Data Quality Campaign. (2014). Safeguarding data: Federal privacy laws that apply to children and education. Retrieved from https://dataqualitycampaign.org/resource/safeguarding-data-federal-privacy-laws-apply-children-education/

2 Data Quality Campaign. (2014). State student data privacy legislation: What happened in 2014, and what is next? Retrieved from https://dataqualitycampaign.org/resource/state-student-data-privacy-legislation-happened-2014-next/

3 Bulger, M., McCormick, P., & Pitcan, M. (2017). The legacy of inBloom. Retrieved from https://datasociety.net/pubs/ecl/InBloom_feb_2017.pdf

4 Tan, S. (2013). After BESE discussion, White pulls student information from database. Retrieved from https://www.nola.com/education/2013/04/after_bese_discussion_white_pu.html

5 A837. Assemb. Reg. Sess. 2013-2014. (L.A. 2014)

6 A677. Assemb. Reg. Sess. 2013-2014. (L.A. 2014)

7 Guidry, L. (2015). School announcing your kid made varsity? That's illegal. Retrieved from https://www.thenewsstar.com/story/news/local/2015/07/26/school-announcing-kid-made-varsity-illegal/30701291/

8 Dreilinger, D. (2014). Education department starts effort to protect student privacy with anonymous IDs. Retrieved from https://www.nola.com/education/2014/06/education_department_starts_ef.html

9 Spradlin, C. & Guidry, L. (2015). School announcing your child made the honor roll? That's illegal. Retrieved from https://www.shreveporttimes.com/story/news/local/2015/07/23/school-announcing-child-made-honor-roll-illegal/30590075/

10 Guidry, L. (2015). School announcing your kid made varsity? That's illegal. Retrieved from https://www.thenewsstar.com/story/news/local/2015/07/26/school-announcing-kid-made-varsity-illegal/30701291/

11 Dreilinger, D. (2014). Education department starts effort to protect student privacy with anonymous IDs. Retrieved from https://www.nola.com/education/2014/06/education_department_starts_ef.html

12 Dynarski, S. (2015). When guarding student data endangers valuable research. Retrieved from https://www.nytimes.com/2015/06/14/upshot/when-guarding-student-data-endangers-valuable-research.html

13 Chuong, C. (2014). Conflicting policy trends shape personalized learning's future. Retrieved from https://aheadoftheheard.org/conflicting-policy-trends-shape-personalized-learnings-future/

14 Herold, B. & Davis, M.R. (2015). 'De-Identifying' student data is key for protecting privacy. Retrieved from https://www.edweek.org/ew/articles/2015/08/26/de-identifying-student-data-is-key-for-protecting-privacy.html

15 Facebook correspondence from John M. Schroder on April 28, 2015. Retrieved from https://www.facebook.com/SchroderLA/posts/these-are-the-five-bills-that-i-have-filed-for-the-2015-legislative-session-thes/865373140197378/

16 U.S. Department of Homeland Security. (2008). Privacy policy guidance memorandum. Retrieved from https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf

17 Guidry, L. (2015). School announcing your kid made varsity? That's illegal. Retrieved from https://www.thenewsstar.com/story/news/local/2015/07/26/school-announcing-kid-made-varsity-illegal/30701291/

18 A228. Assemb. Reg. Sess. 2015-2016. (L.A. 2015)

19 Guidry, L. (2015). School announcing your kid made varsity? That's illegal. Retrieved from https://www.thenewsstar.com/story/news/local/2015/07/26/school-announcing-kid-made-varsity-illegal/30701291/

20 Spradlin, C. & Guidry, L. (2015). School announcing your child made the honor roll? That's illegal. Retrieved from https://www.shreveporttimes.com/story/news/local/2015/07/23/school-announcing-child-made-honor-roll-illegal/30590075/

21 SB89. Assemb. Reg. Sess. 2015-2016. (G.A. 2015)

22 SB275. Assemb. Reg. Sess. 2009-2010. (M.D. 2010)

23 HB358. Assemb. Reg. Sess. 2016-2017. (U.T. 2016)

24 Data Quality Campaign. (2014). Safeguarding data: Federal privacy laws that apply to children and education. Retrieved from https://dataqualitycampaign.org/resource/safeguarding-data-federal-privacy-laws-apply-children-education/

25 National Forum on Education Statistics. (2016). Forum guide to education data privacy. Retrieved from https://nces.ed.gov/forum/pub_2016096.asp

26 Data Quality Campaign. (2014). Student data and consent policies: Avoiding unintended consequences. Retrieved from https://dataqualitycampaign.org/resource/student-data-consent-policies-avoiding-unintended-consequences/

27 Leichty, R. & Leong, B. (2015). De-identification & student data. Retrieved from https://fpf.org/wp-content/uploads/FPF-DeID-FINAL-7242015jp.pdf

28 U.S. Department of Education. (2016). Protecting student privacy while using online educational services: Model terms of service. Retrieved from https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-model-terms-service

29 U.S. Department of Education. (n.d.). Security best practices. Retrieved from https://studentprivacy.ed.gov/topic/security-best-practices

Protecting Students, Advancing Data: A Series on Data Privacy and Security in Higher Education **is a project of the Institute for Higher Education Policy. This report was produced with support from Arnold Ventures. The views expressed in this report are solely those of the authors.**