EDUCATION COMMISSION OF THE STATES

POLICY GUIDE

SEPT **2022**

Lessons in Data Privacy for Education Leaders

Claus von Zastrow and Zeke Perez Jr.

As education data becomes more varied and complex, so do the challenges of protecting students' privacy. By incorporating new data sources, embracing new technologies and reaching new audiences, data systems are becoming more powerful tools for diagnosing and addressing learners' diverse and changing needs. Such advances in data collection and reporting, if not accompanied by comprehensive data privacy policies or data security structures, can also raise the odds of privacy harms, including unintentional or malicious disclosures of learners' private information. Such disclosures can do devastating and lasting damage to people's reputations, life prospects and trust in organizations.

In July 2022, Education Commission of the States assembled data privacy experts and practitioners for a Thinkers Meeting to consider strategies for protecting learners' privacy without compromising the power of education data. Participants focused on the need for coherence and capacity. They called for leaders across state agencies to embrace a common vision for data privacy grounded in consistent policies, coherent data governance structures, continuous capacity-building efforts and clear communication to stakeholders. Such a vision, they said, would support data privacy policies and practices that maximize the benefits of data-driven decision-making while minimizing the risks.

Under the right circumstances, data empower students, families, educators and policymakers to be better decision-makers and advocates. However, violations of privacy can put students and families at risk.

Efforts to protect privacy can fail without a unifying vision for using data in education.

Coherent laws, robust governance structures, effective training efforts and a commitment to transparency can support a unifying vision for education data privacy.

Understanding the Stakes of Student Data Privacy

Participants noted that discussions of data and privacy often come down to power. Under the right circumstances, data empower students, families, educators and policymakers to be better decision-makers and advocates. Violations of privacy can, by contrast, rob students and families of that power, with sometimes devastating consequences for their reputations, opportunities for advancement or financial security.

Defining Data Privacy in Education

Participants in the Thinkers Meeting pointed out that schools and districts must collect sensitive personal data on individual students to provide education services or to comply with federal or state laws. They began the meeting by defining the scope of their discussion: Which data requires protection, whose data requires protection and what mechanisms do leaders have to protect this data?

Which data requires protection? Laws and policies typically define data requiring protection as personally identifiable information (PII), or information stored in education records that can be used to identify an individual. Such information can include direct identifiers (such as names or unique student IDs) or indirect identifiers (such as birthdates or gender) that, in combination, can reveal an individual's identity. This brief will refer to PII as "student data."

Whose data requires protection? The meeting focused on the need to protect information about learners at all levels: from early childhood through adult education. Though participants said information about teachers and other school staff also requires protection, they determined that such information was beyond the scope of their discussion, because education privacy laws do not typically address it.

What mechanisms protect data? Participants addressed behaviors as well as systems that can protect student data. Policies that regulate the behavior of those who handle student data can prevent inadvertent or malicious violations by limiting who has access to student data, how it can be shared, how it can be used, how it must be secured or when it must be destroyed. Secure data systems employ technology and controls that can help prevent unauthorized access to, or theft of, data.

Recent data breaches affecting millions of students have grabbed headlines, but even unintentional disclosures of student data that result from negligence or weak data-sharing protocols can cause harm. Private information like disciplinary records, test scores or health assessments can cause lasting reputational damage if it becomes public, limiting students' access to education and job opportunities or causing emotional distress. There are also equity implications for people dealing with data privacy concerns, because those with less social or financial capital may be most affected by data privacy infractions.

One important aim of data privacy laws and policies is to give parents certain rights to their children's data, which pass to children themselves when they turn 18 or enroll in a postsecondary institution. Participants argued that those rights can empower parents and students to take more control over their future.

Mounting Challenges to Protecting Data Privacy

Participants maintained that limited resources for education data privacy and security efforts, together with new technologies and mounting demands for information, have made it harder to strike a balance between the benefits of data and the dangers of privacy violations. Schools increasingly share data with after-school partners; state education agencies exchange data with other state agencies; third-party vendors collect student data; and some schools and colleges use online surveillance systems that scour students' social media for threats.

Participants pointed out that the pandemic accelerated the pace of such changes, propelling millions of students onto virtual learning platforms, turbocharging the adoption of education technology, compelling schools and colleges to track student COVID-19 infections, requiring education and health agencies to share data, and prompting some schools to screen students for mental health challenges.

Education leaders found themselves responsible for such private information as images of students' homes captured by web cameras, data gathered by hastily adopted learning apps, and information collected on students' emotional state. Educators and leaders had little guidance on how to apply existing data privacy requirements to changing contexts and an often imperfect grasp of the privacy risks involved.

The nation's political climate can exacerbate these challenges. Participants noted that privacy touches on many sensitive political and cultural issues, including distrust of government, suspicion of commercialism, parents' access to information about their children's preferred pronouns, and debates about surveillance measures to prevent school shootings. In this climate, participants cautioned that high-profile violations of privacy could spark a broad backlash against data collection and reporting in general, undermining even the basic need to measure and improve educational outcomes.

Actionable Approaches to Support Data Privacy

When discussing how state policymakers can support data privacy in this challenging environment, meeting participants alluded to a widely quoted maxim: "Vision without action is a daydream, but action without vision is a nightmare." Much of their discussion focused on the balance between vision and action. They urged state leaders to maintain a coherent vision for privacy as a safeguard against the uncertainty and confusion that undermines so many well-intentioned privacy policies. They also recommended actions that support the vision — including coherent laws, robust governance structures, effective training efforts and a commitment to transparency.

A Coherent Vision

Participants maintained that state leaders should create a coherent and sustaining vision for education data privacy. Several cited the Student Data Principles, a consensus document endorsed by 41 organizations, as a useful model for such a vision. Without a unifying vision for using data in education, efforts to protect privacy can be weak, ad hoc, contradictory or reactive. Educators might collect data they don't need or use data in ways no one could have anticipated, multiplying threats to privacy. When threats become apparent or violations occur, participants argued, leaders under pressure to respond may hastily pass laws that could have unintended consequences, conflict with prior laws and create confusion — all while doing little to improve the overall privacy and security of students' private information.

Considerations for State Leaders

When considering tenets that should be central for a data system's vision, participants offered the following guidance:

Lead with the benefit. Any vision for data privacy must first articulate the purpose of data systems: to benefit individuals and society. Data about any individual should first and foremost support that individual.

Find a prominent and influential champion. Governors, agency heads, state school board presidents and prominent legislators can be powerful messengers for a vision of data privacy. A vision is more likely to resonate if it comes from leaders who command a bully pulpit, convening power, authority to make decisions and the ability hold people accountable.

Build on governance structures. Governance and vision are often intertwined. Strong governance structures can be a vital foundation for an ambitious and actionable data vision. (For more on governance structures, see the governance structures section.)

State Examples

The Center for Statistics begins its Security and Privacy page by asserting the value of data. KYSTATS, which links data from multiple state education and workforce agencies, exists to "collect, link and evaluate education and workforce data so that Kentucky's leaders, policymakers and the public can have the facts to make the best decisions for our state." The page then describes how it accomplishes that overarching goal by de-identifying data, suppressing information that can compromise individual students' privacy and employing strict security standards.

The Education Research & Data Center's Vision, Mission and Values page presents a unifying vision for the value of data that weaves in data privacy. The ERDC's Data Privacy Practices document outlines detailed information about the center's privacy priorities, which include data minimization, transparency, accountability and security.

Coherent Laws

Meeting participants agreed that coherent and well-implemented data privacy laws can help leaders enforce their vision. They observed that the current maze of state and federal student data privacy laws can confuse those who must abide by them. Many of those laws are duplicative with existing federal requirements, and some are contradictory. They can be vague or indiscriminate, unintentionally prohibiting strategies or tools schools need. For example, sweeping biometric laws could ban school-supplied devices, which increasingly include fingerprint readers. All too often, participants said, new privacy laws fail because they lack official guidance, funding or enforcement. In addition, states seldom revisit laws that fail to keep pace with new technologies or needs that can open new avenues for privacy violations.

Considerations for State Leaders

Participants shared several considerations for state leaders on data privacy laws:

Conduct due diligence. Before recommending or conceiving new laws, governors and legislators should ask critical questions: Is the proposed law necessary, or do other laws already cover the same territory? Does it conflict with prior laws? Does it define its terms carefully? Does it account for unintended consequences? Most important, does the proposed law advance or impede the state's vision for data use and privacy?

Foster effective implementation. After a law passes, state leaders can do more to foster effective implementation. Regulatory authorities, such as the state attorney general, can disseminate clarifying regulations; and agency heads can design more detailed agency policies and procedures for implementing the law. Legislators should fund the laws, so that other state and local leaders can afford to implement them through efforts like upgrading security infrastructure, hiring data privacy and security personnel, or training staff and teachers. Finally, leaders must enforce the laws, or the laws will have little impact.

Renew obsolete laws. Over the long term, state leaders can work with educators and education technology leaders, privacy experts, parents and even vendors to revisit and renew data privacy laws. For example, they may consider such questions as: Do existing laws take new technologies and data needs into account? Do they conflict with new federal or state requirements? Have they been enforced? Have they had a positive impact on student privacy?

Federal and State Data Privacy Laws

Meeting participants recognized that state and local leaders must navigate a complex set of federal and state privacy laws. They argued that two of the most important federal laws addressing current challenges are the Family Educational Rights and Privacy Act of 1974 (FERPA) and the Protection of Pupil Rights Amendment (PRPA).

- FERPA, which is a foundation for many subsequent state laws and policies, gives parents the right to access their children's education records, seek amendments to those records and exercise some control over how those records are disclosed. When a student turns 18 or enters a postsecondary institution — whichever comes first — those rights transfer to the student.
- PPRA governs implementation of surveys, analyses or evaluations that address protected areas, such as political affiliations, mental disabilities or health diagnoses, sexual behaviors, religious practices or affiliations, or criticism of family. The law is growing more important as more districts and schools field surveys to assess students' mental or emotional health.

Other federal laws that govern children's privacy include the Children's Online Privacy Protection Act, which applies to vendors, and the Individual with Disabilities Education Act, which offers additional privacy protections for students who receive special education services.

Participants noted that efforts to track student infection rates during the pandemic require school leaders to understand the intersection between Health Insurance Portability and Accountability Act and FERPA.

For guidance on these and other federal laws, follow links to the U.S. Department of Education's Privacy Technical Assistance Center, the Consortium on School Networking's protecting privacy toolkit and resources for policymakers on Student Privacy Compass.

The landscape of state privacy laws is still more complex. Participants noted that states have enacted more than 130 privacy laws, creating a challenging regulatory environment for education leaders.

State Examples

The conversation continued as leaders shared examples of state laws that embody some of their recommendations:

H.B. 245 created a Student Data Privacy Council to review the implementation of the state's Student Data Privacy Act of 2015, study other states' laws, consider the impact of technology developments, and recommend any appropriate statutory or regulatory changes to the governor and General Assembly. Among the recommendations in the council's January 2021 report: clarify definitions, strengthen enforcement and improve transparency. Maryland H.B. 769 adopted some of the new definitions and reauthorized the Student Data Privacy Council.

H.B. 358 created a state data governance structure and appointed a student data officer to promote a more coherent data privacy infrastructure across the state. It also required each district to form its own data governance policies and designate a student data privacy manager to build local capacity for data protection. In addition, it established an advisory group of district and school data users who offer input into the feasibility of proposed data policies.

Governance Structures

A portion of the meeting focused on data governance, which defines the roles and responsibilities that ensure clear processes for collecting education data, reporting on it, promoting its quality and maintaining its security. A compelling vision for data privacy relies on strong governance to carry it out. Participants maintained that education data governance structures and policies are insufficient in many states, both in single agencies and in statewide longitudinal data systems that involve multiple agencies. That challenge is especially acute in some states' SLDS governance structures, which, participants agreed, can be weak or nonexistent. Different agencies or offices in agencies can maintain data silos with inconsistent privacy controls and regulations, which can inhibit data-sharing or lead to unauthorized disclosures.

Considerations for State Leaders

After discussing how important state governance structures are for implementing data privacy laws, attendees offered several ideas for state policymakers to consider:

Create and implement a formal governance structure. At a minimum, governors and agency leaders can ensure that a data governance structure exists for any single-agency or cross-agency data system. The structure should clearly define roles, responsibilities, operational decision-making structures and processes that protect the privacy of student data.

Incorporate existing structures. Where possible, state policymakers should take stock of and incorporate existing governance policies and practices, both formal and informal. Simply sweeping away existing structures can breed disaffection and confusion, undermining efforts to protect privacy.

Make governance structures actionable. To be successful, it's important that governance policies include clear and enforceable procedures, along with support for staff who need to carry them out. Actionable governance structures include procedures for sharing data, auditing and correcting data privacy practices, and reporting and responding to security breaches. Support for agency leadership and staff, including training in their respective roles and responsibilities, can clarify these procedures while giving the governance structure staying power.

Build governance structures for the long term. Participants noted that governance structures required to build a data system may be different from the structures needed to maintain it. Governors, legislators and agency leaders may need to revisit governance structures after they stand up a system.

State Examples

The 2019 Cradle-to-Career Data System Act established a governing board that includes leaders from agencies representing education, workforce development, and health and human services, as well as legislators and members of the public. Such cross-agency governance structures can support common data-sharing protocols that minimize risks to student data without blocking the flow of data.

The Office of Superintendent of Public Instruction outlines comprehensive data-sharing processes and policies for student-level data requests. The document guides data sharing across state agencies and includes specific approval criteria for protecting student data.

Training

Coherent laws and governance structures will have little impact, participants insisted, without comprehensive, adaptable and recurring training for leaders, teachers, parents, students and anyone else who handles education data. Training helps these stakeholders understand and carry out their respective roles to form a cohesive system. Participants agreed that a lack of training in data privacy and security only compounds problems with implementation. Many data users don't understand which data should be protected, why it should be protected or how to do so. Often, districts and schools squeeze privacy guidance into brief IT training sessions that educators receive only once a year.

Considerations for State Leaders

State leaders can support training by focusing on three priorities: compulsion, capacity and quality.

Compulsion. Participants said that data privacy training should be required by law. The Individuals with Disabilities Education Act already requires privacy training for anyone who handles data of students with disabilities, and legislators could extend such training requirements to those who handle any student's data. Legislation could require privacy training in educator preparation and professional development programs, for example.

Capacity. Participants pointed out that compulsion would do little good without support, such as funding and technical assistance for state and local leaders. Educators are required to take part in a growing number of training exercises each year, many of which naturally get cut short. While legislators can provide funding for more substantial training, agency leaders can provide training materials, help local leaders tailor those materials to their needs, and offer avenues through which teachers and other data handlers can ask practical questions about implementation.

Considerations for State Leaders continued

Quality. The group agreed that effective data privacy training should be early, embedded in other preparation and training, ongoing, adaptable and relevant. P-12 and higher education leaders can include it in educator preparation programs and integrate it into routine professional development efforts. States should also ensure that training adapts to the very diverse roles and needs of those who interact with student data: from the front office managers who handle student data to the classroom teachers who use it to inform their teaching strategies. Such efforts to make training relevant can reduce the burden on educators by tailoring their responsibilities to their roles.

State Examples

The data privacy law requires any public school employee with access to student data to complete training on student privacy laws in order to receive certification to use education records. The Utah State Board of Education requires the Utah Student Data Privacy Educator Course for all educators renewing their license in the state.

The Department of Public Instruction offers a suite of student data privacy training materials addressing such topics as protecting student data, understanding and managing different types of student records, sharing information across systems and complying with federal law. The materials include videos and a training module users can follow at their own pace.

Transparency

Meeting participants stressed that state leaders can foster a culture of transparency regarding data use and privacy. Transparency promotes public trust in data systems by helping students, parents and other involved parties understand why data are important and how agencies or schools use them. Truly transparent data systems help students and their families understand — and act on — their rights over their personal data. Participants agreed that some state agencies provide too little information about data privacy policies and commitments, while others provide a flood of complex information few people have time to read. Many, they said, do too little to ensure that families or students know what to do with the information they receive.

Considerations for State Leaders

Participants offered suggestions for how state leaders can encourage meaningful transparency:

Make the information available. As a good first step, agency leaders can ensure that data privacy policies are readily available on their websites. At least 31 states publish formal data privacy policies for their statewide longitudinal data systems. In addition to explaining how their systems comply with federal or state laws, those policies often include information on what kinds of data the state collects, who has access to that data, how the state shares the data among agencies, how it stores the data and when it destroys the data. It's also important for agency leaders to be transparent with other state leaders, such as governors and legislators, about changes to data collection and use that might affect privacy policies.

Make the information understandable. Data privacy policies can be dense, so leaders of state agencies should prominently publish brief summaries of their data privacy policies that focus on their purpose. Those summaries can then orient readers to a menu of documents on more specific topics.

Make the information actionable. State leaders can offer — and widely publicize — customer support lines so that state residents can ask questions, receive guidance or alert leaders to privacy violations. In addition, agency leaders can very clearly describe the trade-offs parents or students must consider if they exercise their rights to opt out of certain types of data collection. To opt out of data collection may be to opt out of services or extracurricular opportunities, for example.

State Examples

The Student Data Privacy, Accessibility, and Transparency Act includes requirements to inform the Legislature and the public on data use and proposed changes for any new data collection. The law also requires a report to the Legislature to note who data is being shared with, for what purpose and for how long.

P-20 to Workforce Research Data System prominently publishes a privacy pledge that describes the system's aim to "balance privacy with the ability to discover insights about Nevada's education, higher education, and workforce policies, initiatives, and programs." The page describes the system's key privacy protections and dispels what it describes as myths about systems' purpose and operations.

Final Thoughts

Throughout the Thinkers Meeting, participants acknowledged that it is not easy to maximize the benefits of data systems while keeping possible harms at bay. New data sources and technologies bring both promise and peril, and some threats to student privacy might not be immediately apparent. Laws and funding structures don't always keep pace with rapid change. Still, participants maintained that a consistent vision, supported by efforts to continually revisit and renew the policies that support that vision, can help state leaders strike the best possible balance.

Thinkers Meeting Participants

Education Commission of the States Thinkers Meetings convene national education leaders to identify best practices states can adopt to improve education. This report does not present a consensus among all the participants in the meeting. Rather, it offers an overview of the meeting's major themes and recommendations.

Participants

Rachel Anderson, vice president, Data Quality Campaign
Linnette Attai, president, PlayWell, LLC
Marcia Bohannon, chief information officer, Colorado Department of Education
Sean Cottrell, director, WestEd
Dean Folkers, director of education data and technology, Council of Chief State School Officers
Ross Goldstein, executive director, Maryland Longitudinal Data System Center
Kate Lipper-Garabedian, state representative, Massachusetts House of Representatives
David Sallay, chief privacy officer, Utah State Board of Education
Jim Siegl, senior technologist, The Future of Privacy Forum
Amelia Vance, president, Public Interest Privacy Consulting
Levette Williams, subject matter expert, AEM Corp

Education Commission of the States Staff

Zeke Perez Jr., senior policy analyst, Education Commission of the States
Claus von Zastrow, senior policy director, Education Commission of the States

About the Authors

Claus von Zastrow

As a senior policy director, Claus works with his Education Commission of the States colleagues to promote timely and relevant education policy and research. He has held senior positions in education organizations for more than 20 years and has spent much of that time helping diverse stakeholders find consensus on important education issues. Claus is dedicated to ensuring that state leaders have the information and guidance they need to make the best possible decisions affecting young people. Contact Claus at cvonzastrow@ecs.org.

Zeke Perez Jr.

As a senior policy analyst, Zeke tracks legislation related to statewide longitudinal data systems, school safety and postsecondary campus safety. He has been with Education Commission of the States since 2014. Zeke has a passion for local politics and enjoys following the varied policy approaches of city and state leaders. Contact Zeke at zperez@ecs.org.

Acknowledgments

This report is based on research funded by the Bill & Melinda Gates Foundation. The findings and conclusions contained within are those of the authors and do not necessarily reflect positions or policies of the Bill & Melinda Gates Foundation.