Foundation for Excellence in Education

DECEMBER 2015

PROTECTING K-12 STUDENT PRIVACY IN A DIGITAL AGE

ABOUT EXCELINED

Founded by former Florida Governor Jeb Bush, the Foundation for Excellence in Education is igniting a movement of reform, state by state, to transform education for the 21st century economy by working with lawmakers, policymakers, educators and parents to advance education reform across America. Learn more at ExcelinEd.org.

FOR INFORMATION ON STUDENT DATA PRIVACY POLICY

Special thanks to Douglas Levin, Founder and President of EdTech Strategies, LLC for his research and writing for this paper. If you have any questions, need assistance or more information on developing a Student Data Privacy Policy in your state please contact Neil Campbell, Director, Next Generation Reforms.

EXCELINED.ORG

E INFO@EXCELINED.ORG

@EXCELINED

P 850.391.4090

FACEBOOK.COM/EXCELINED

Table of Contents

EXECUTIVE SUMMARY

The last decade has seen many exciting innovations in education. Educators have developed new instructional models that accelerate and deepen student learning by tailoring instruction to each student's individual needs, skills, and interests. This personalization will require technology to help educators monitor student progress and communicate with families, as well as to help students interact with online content and collaborate with each other. There can be little argument that ensuring the privacy and security of all this student data is a critical issue that needs to be addressed in this move towards a more personalized education system. In fact, about 4 in 10 parents (41 percent) are either very or fairly concerned about the collection of data about how much students are learning from assignments completed using new education technology tools. While the issue may not be top of mind for most education policymakers, a single incident – such as a news article exposing a concerning privacy practice or data breach (even beyond the K-12 education context) – has the very real possibility of dramatically increasing calls on policymakers to take immediate action to protect students.

In recent years nearly every state in the nation has responded by considering new student data privacy legislation to build upon the aging foundation offered by federal law and to meet the unique circumstances and needs of their schools and communities. Given the complexity of the issue and its relationship to the implementation of other important education policies, it is important for policymakers to ensure that their actions effectively address parents' privacy concerns without unintentionally undermining schools' ability to provide students the personalized, high-quality education parents expect and that will prepare students for success in college, life, and work.

While many states have taken positive approaches to addressing these challenges, there have a number of legislative proposals that have struggled to strike the right balance among these factors. In response, ExcelinEd has taken a leadership role in actively providing support to state policymakers as they work to modernize outdated laws and respond to the concerns of parents by advancing comprehensive, balanced student data privacy protections. Most notably, ExcelinEd developed and in 2015 updated the *Student Data Privacy, Accessibility and Transparency Act*, which is a model policy designed to provide the most comprehensive protections presently available in state law to ensure student data is used responsibly. This updated model policy was a starting point for legislators in Georgia in what became Senate Bill 89 that was passed into law unanimously in both chambers and signed by Governor Nathan Deal. In addition to comprehensive and updated definitions of important terms and legislative intent, the model policy updates, extends, and enhances existing federal privacy protections and directly aligns with internationally recognized privacy best practices.

Targeted to state policymakers and their advisors and grounded in new data commissioned by ExcelinEd on parent views about technology and student data privacy, the purpose of this paper is threefold:

1. to shed light on the context for the privacy of student data as an issue and on parental concerns more specifically;
2. to provide a brief review and analysis of the current federal and state legislative landscape regulating the collection and use of data about students; and,
3. to suggest potential strategies for addressing outstanding parental and public concerns, including via the passage of new state legislation.

The paper concludes with recommendations of actions that various stakeholders – including state education agencies, school districts, parents, and companies – can take even in the absence of the passage of new legislation to improve student data privacy and security in the current K-12 context. With or without new legislation, protecting student data will require a focus on good governance processes, regular review of security practices, transparency and effective communications, and a commitment to build the capacity of state, district and school level employees to protect student data.

STUDENT SAFETY AND WELFARE IN A DIGITAL AGE

While the primary mission of elementary and secondary schools is to prepare all students for success in further education, life, work, and citizenship, we also expect schools and educators to ensure the safety and welfare of the children and youth entrusted into their care. Whether taking action to protect students from extreme weather, outbreaks of disease, natural disasters, or the rare actions of those actively seeking to harm children, this duty of care expectation has both a legal and moral grounding.

Of course, neither schools nor the potential risks facing students are unchanging. For instance, schools across the nation are increasingly relying on technology for the delivery of core education programs and services, such as for textbooks and tests and for communicating with parents. While this use of technology has many benefits, most especially with helping educators to personalize instruction to meet the individual and unique needs of children, policymakers, educators and parents must remain cognizant of the ways in which our use of the technology may at the same time represent potential new risks for students and school communities.

For years, schools have been responding to some of these new technology-related risks, including with respect to cyber-bullying and Internet safety.[1] In recent years, however, additional privacy-related concerns have risen to prominence related to the extent of information collected about students in school via technology and how that digital information may be used today or at some time in the future in ways that could exploit or even harm students.

The sections that follow shed additional light on the issue of privacy in education, including why it has emerged as an issue in recent years and strategies to address parent concerns, all grounded in new data commissioned for this paper by ExcelinEd on parent views about technology and student data privacy.

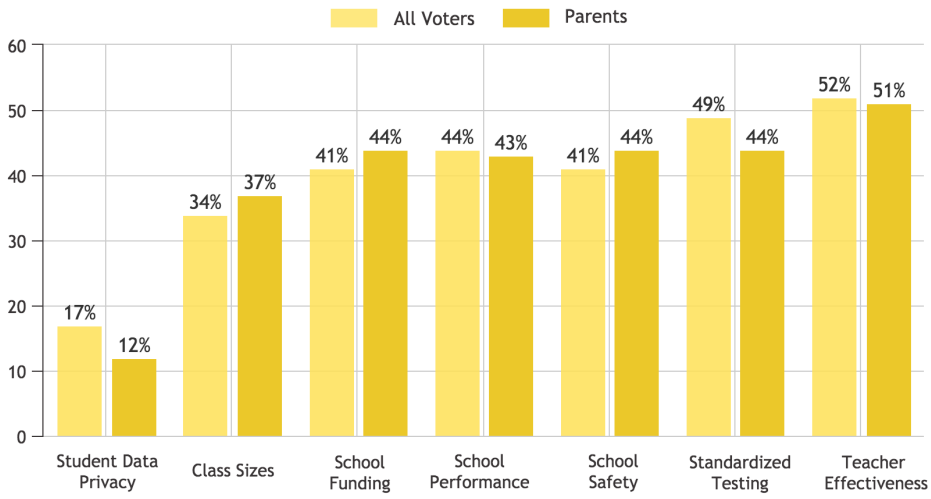
Why Privacy Has Emerged as an Issue in Education

Like many issues of public policy, the calls for action by advocates to address issues of student data privacy can feel like they are directly and disproportionately linked to breaking news stories and headlines (and the intense reaction to those stories on social media). An event- and media-driven approach to policymaking, however, can distort measured assessments of the root causes of issues, reduce the odds of identifying effective solutions, and introduce unintended consequences in responses.

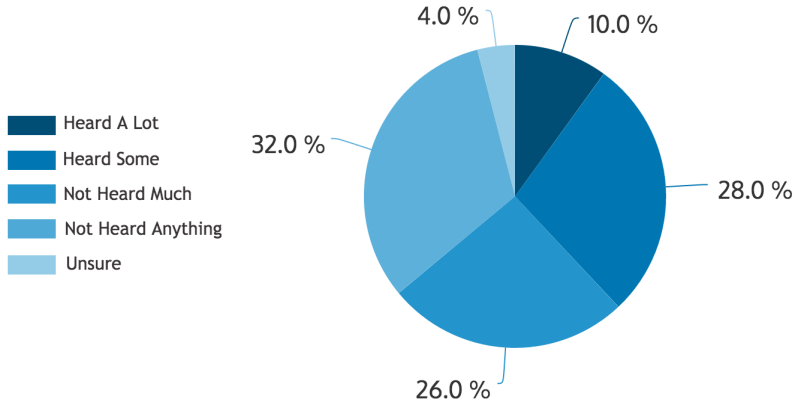
Polling data, in fact, suggest privacy is not currently a top-tier concern of parents or the general public when thinking broadly about the range of issues facing K-12 education. Nonetheless, it remains a critically important issue facing policymakers, school and industry leaders, and parents alike. There are at least three reasons the issue of privacy in education has emerged in recent years as an issue.

STUDENT DATA PRIVACY IN CONTEXT

BIGGEST CONCERNS FACING PARENTS OF STUDENTS IN PUBLIC SCHOOLS



MAJORITY OF PARENTS HAVE NOT HEARD OF STUDENT DATA PRIVACY AS AN ISSUE



First and foremost, there have been a series of high-profile breaches of corporate, government, and consumer information in sectors *beyond* education, from the 2015 hacking of Office of Personnel Management federal employment records to the 2014 malicious leaking of private Sony emails and documents to the stealing of consumer credit card data from Target

in late 2013. Together these incidents, and others like them, have served both to raise awareness by policymakers and the general public about the sheer amount of information collected and stored about individuals in computer systems as well as to erode trust in our ability to adequately secure that digital data from prying eyes.

Second, while the headline grabbing data privacy breaches haven't occurred in K-12 education like they have in other sectors, school districts and providers haven't been immune from their own technology-related privacy concerns as they increasingly transition to the use of digital instructional tools and services.[2] Indeed, concerns about privacy and student data collection that were not transparently addressed were instrumental in the winding down in 2014 of the non-profit educational data management service inBloom, which strove to facilitate data sharing among states, districts and vendors. More recently, Natasha Singer of the *New York Times* shed light on another case in point: the state of data security practices among companies serving the K-12 education sector by highlighting the insufficiency of encryption practices employed by education companies that had voluntarily signed a national pledge to safeguard student privacy.[3]

Finally, issues of data privacy and security also have been conflated with disagreements about state and federal education policy, especially with respect to testing and accountability policy. For instance, in response to concerns raised by advocates about online testing by the Partnership for the Assessment of Readiness for College and Careers (PARCC) and the Smarter Balanced Assessment Consortia, the Federal Trade Commission (FTC) itself weighed in on this issue in January 2015. The FTC clarified the responsibility of various actors under the federal *Children's Online Privacy Protection Act* (COPPA) to protect children's privacy with respect to online educational services used by and under the direction of school districts and states (who themselves are acting under state and federal legislative mandates). In so doing, the FTC underscored that COPPA was not designed to 'displace the traditional relationship between parents and schools when it comes the collection of information exclusively for educational purposes in the school context and with the school's permission.'[4] Nonetheless, protecting the privacy and security of information about students remains a work in progress with roles to be played by many actors, including states, school districts, education companies, and parents.

In sum, there can be little argument that ensuring the privacy and security of student data is a critical issue that needs to be addressed in the move to personalized education. While the issue is not top of mind for most parents, a single incident – such as a news article exposing a concerning school district or technology company practice or data breach (whether or not the issue is even education-specific) – has the very real possibility of dramatically increasing calls on policymakers to take immediate action to protect students. Given the complexity of the issue and its relationship to the implementation of other important education policies, it is important for policymakers to ensure that their actions adequately address parents' privacy concerns without unintentionally undermining schools' ability to help prepare students for further education, life, work, and citizenship in an increasingly technology-driven world.

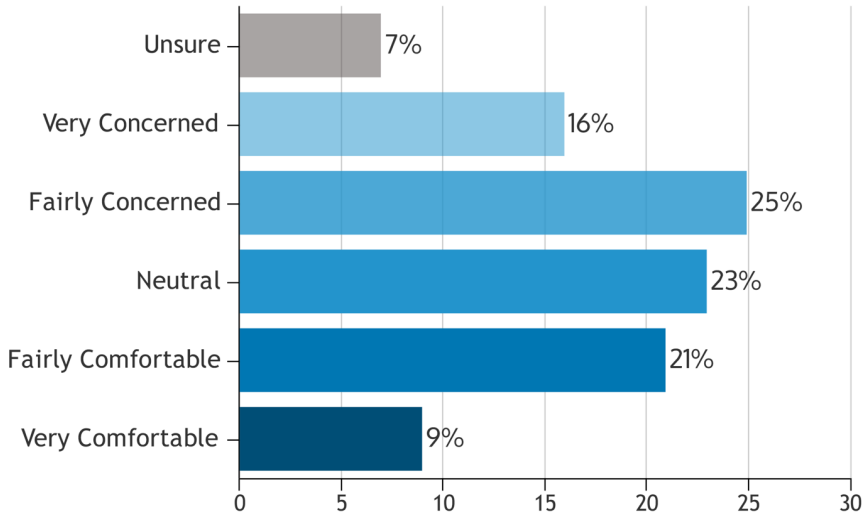
Understanding Parent Views About Technology and Privacy

In order to gain a more concrete understanding of what parents want to know about data privacy, in May 2015 ExcelinEd commissioned Echelon Insights to conduct a National Public Opinion Research Study of 800 individuals nationwide, 350 of which were parents of a K-12 student. While parents' views about the role of technology in education continue to evolve, a majority of parents are and continue to be supportive of digital learning. According to ExcelinEd's study, a majority (55 percent) of parents believe that the use of new technology and software in the classroom that allows students to do things like complete assignments and tests is a good or very good thing. An even larger majority of parents (nearly 2 of every 3 parents) are in favor of using technology in more innovative ways in the classroom, such as by helping teachers to better personalize their instruction for students.

At the same time, a sizeable proportion of parents (41 percent) express at least a general level of concern about the collection of data about students and student learning that accompanies the use of this new technology and software.

When the ExcelinEd study probed that concern by eliciting reactions from parents to hypothetical (but realistic) data collection and sharing scenarios, parents tended to report greater privacy concerns in the cases where data collections may include information beyond strictly academic learning measures (such as when data is collected about student discipline, race, disability, or poverty) and when those same data were used for purposes other than directly supporting teachers to help students learn, especially when the data was shared with individuals and organizations outside the school and district. The highest levels of concerns reported by parents in these hypothetical scenarios involved situations where schools shared non-academic data with technology companies to help them improve the tools and software they provide to schools.

Parent comfort with collection of data about how much students are learning from assignments completed using new education technology tools.



In an effort to garner more specific information about the types of questions and concerns parents may have about the privacy of student data, the ExcelinEd study also asked parents

about questions they may have for school districts about the issue. Parents reported that their most important questions included:

1. Who has access to this student learning data?
2. What laws are in place to protect student data privacy?
3. How is the data being protected and kept secure?
4. What type of data is being collected about student learning?
5. What can companies use the data for?

Parents' priorities clearly seem to be directed at understanding the boundaries and protections in place to safeguard information collected about their children, especially when that information may be shared with those beyond their own school district.

THE PROMISE OF PERSONALIZED LEARNING

The goal of personalized learning is to accelerate and deepen student learning by tailoring instruction to each student's individual needs, skills, and interests.[5] *While an increasing number of schools are pursuing varied approaches to meeting this goal, some of the most successful programs focus on blending online learning with other traditional learning experiences, including providing each student with some element of control over the time, place, path, and/or pace necessary to mastering curricula aligned to challenging state academic content standards.*[6]

According to research compiled by the Evergreen Education Group and the Clayton Christensen Institute for Disruptive Innovation, Horry County Schools in Conway, South Carolina, for instance, launched their district-wide Personalized Digital Program in the 2013-14 school year to foster student ownership of learning and maximize academic learning time. Although still relatively new, the program is already starting to see results in math and reading as assessed by Northwest Evaluation Association's Measures of Academic Progress.[7] *Similarly, the Spokane Public Schools in Spokane, Washington has implemented blended learning models in numerous programs across the school district (in concert with other initiatives), resulting in a rise in the district's graduation rate from 60 percent in 2007 to 83 percent in 2014.*[8] *And, in Washington, D.C., the District of Columbia Public Schools have recorded extensive and well-studied gains in math and reading since implementing blended learning.*[9]

For policymakers, therefore, it is important to ensure that efforts to better protect student data from unauthorized access and misuse do not unintentionally undercut innovative education programs like these being implemented to meet local community needs across the nation.

Strategies to Address Privacy Concerns of Parents

While the data from this 2015 study shows that issues of student data privacy and security are neither well understood nor necessarily an everyday concern of most parents (except when a public incident focuses their attention on the issue), when probed, parents do reveal consistent, common sense views about their outstanding fears and questions.

While states, school districts, and technology companies are currently taking a range of approaches to addressing the issues of student data privacy and security – some more effectively than others – parents report they are most interested in strategies that focus on parental control and data protections, including by:

- Restricting what information is collected about their child or who has access to it;[10]
- Requiring schools to communicate clearly with parents in writing about what student data is collected and how it is stored, used and shared;
- Requiring schools to develop and implement data security plans to protect confidential information; and
- Providing legal protections that impose strict penalties on schools that misuse or compromise student education data.

In the next section of this paper, the current landscape of federal and state data privacy laws are reviewed and recommendations are made for further state legislative consideration, grounded in privacy best practices and the expressed concerns of parents. The paper then concludes with recommendations of actions that various stakeholders – including state education agencies, school districts, parents, and companies – can take even in the absence of the passage of new legislation to improve student data privacy and security in the current K-12 context.

THE CURRENT LANDSCAPE OF STUDENT DATA PRIVACY LAWS

Federal education privacy laws – the first of which were enacted 40 years ago –provide a foundation (albeit dated) of protections for all students and their families. While the U.S. Congress is currently considering several competing ideas to update or enhance these laws, many states have taken the initiative to update and enhance baseline federal policy protections through the enactment of new state legislation. In the sections below, an overview of major federal student data privacy legislation and highlights of state student data privacy legislation is provided, including details on notable legislative proposals that are or have been considered.

Federal Student Data Privacy Legislation

Three federal laws are primarily responsible for providing a national foundation of privacy protections for students: the *Family Educational and Privacy Rights Act*, the *Protection of Pupil Rights Amendment*, and the *Children's Online Privacy Protection Act*.

First enacted in 1974 and regulated by the U.S. Department of Education, the *Family Educational and Privacy Rights Act* (FERPA) has been updated by federal policymakers via legislative or regulatory amendments nine times in response to new circumstances, including most recently in late 2011. FERPA obligates schools that receive federal funds to establish and follow a set of privacy practices with respect to the collection and sharing of personally identifiable information about students. It also grants a number of important rights to parents (or students themselves, if they have reached the age of 18 or are attending a postsecondary institution) that provide some control over what personally identifiable data can be collected and shared about students.

School Obligations under FERPA	Parent Rights under FERPA
Obligation to inform parents annually of their right to review their student's education record	Right to review their child's education records
Obligation to establish a process for parents to review and seek to amend their student's record	Right to have school amend their child's record, if it is inaccurate, misleading, or otherwise in violation of a student's privacy
Obligation to inform parents annually of the types of personally identifiable information that could be publicly released as school directory information	Right to be informed about the types of personally identifiable information schools could publicly release as directory information about their child

School Obligations under FERPA	Parent Rights under FERPA
Obligation to provide parents an opportunity to opt out of having any or all school directory information about their student publicly disclosed	Right to opt out of public disclosures of any or all school directory information about their child
Obligation to seek parental consent in advance for the disclosure of personally identifiable data for any purpose not authorized in law	Right to opt out of the disclosure of personally identifiable information about their child for any purpose not authorized in law

FERPA further defines the circumstances when a school is legally authorized to disclose the personally identifiable information of its students. For instance, FERPA authorizes the release of personally identifiable student data:

- to other school officials for educational purposes;
- to volunteers, contractors, consultants, and other third parties for the provision of an education service that would otherwise be provided by a school's employees, provided the use of personally identifiable student data remains under the direct control of the school;
- for cases where a student transfers or applies to another school;
- in connection with financial aid;
- for purposes of school accreditation;
- to authorized federal, state and local officials;
- for authorized research purposes; and
- in connection with a health or safety emergency.

In 1978, federal policymakers further expanded the privacy protections provided under FERPA through passage of the *Protection of Pupil Rights Amendment* (PPRA). PPRA grants additional rights to parents (or students themselves, if they have reached the age of 18), including with respect to federally supported student data collections about sensitive topics, the right to receive advanced notification about marketing surveys and the administration of certain physical examinations to students, and the right to inspect instructional materials. Specifically, under PPRA, no student is required to participate in any federally supported survey, analysis or evaluation including any or all of the following sensitive topics without the prior consent of a parent:

- political affiliations or beliefs of the student or the student's parent;
- mental or psychological problems of the student or the student's family;
- sex behavior or attitudes;
- illegal, anti-social, self-incriminating, or 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;
- religious practices, affiliations, or beliefs of the student or students parent; or
- income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

Enacted in 1998, the *Children's Online Privacy Protection Act* (COPPA) is the most recent of the three primary federal student data privacy laws enacted by Congress. Unlike the FERPA and PPRA, both of which are regulated by the U.S. Department of Education and principally address the obligations of schools, COPPA is administered by the Federal Trade Commission (FTC) and principally addresses the obligations of operators of commercial websites, online services, and 'apps' targeted to children (including those whose purposes are not educational). Among other obligations, COPPA requires operators of sites and services that knowingly collect, use, or disclose personally identifiable information about children under 13 – provided directly by children themselves – do so if and only if they first obtain verifiable parent consent. In cases where the use of any such sites, services, or apps are educational, do not involve the collection of personally identifiable information for any other commercial purpose beyond the provision of educational services, and occur at the direction of a school or teacher, COPPA provides that a school can consent to the collection of personally identifiable information on behalf of the parent.

State Student Data Privacy Legislation

In recent years nearly every state in the nation has considered new student data privacy legislation to build upon the aging foundation offered by federal law and to meet the unique circumstances and needs of their schools and communities. According to the Data Quality Campaign, 110 student data privacy bills were considered in 36 states during 2014 state legislative sessions and over 180 have so far been considered in 2015 in 46 different states. This extraordinary state legislative attention has resulted in the passage of more than 50 new state student data privacy laws in the last two years alone.

A May 2015 Foundation for Excellence in Education report, "*Building a Trusted Learning Environment: A Snapshot of State Laws on Student Data Use, Privacy and Security,*" offers an overview of the common elements of many of these new laws, as well as illustrative provisions. Among other findings, the report reveals that within the last two years alone:

- 29 states have supplemented federal definitions of student data, student records, and other key terms in state statute;
- 25 states have outlined data storage and security processes for student data;
- 23 states have delineated comprehensive lists of specific data elements about students that can and cannot be collected;
- 23 states have addressed the use of school or student data by non-public third parties, including vendors;
- 17 states established new requirements for contracts with third parties with regard to student data;

- 8 states have instituted a complaint process for students and parents to address student data privacy violations or a mechanism to design such a process; and,
- 3 states have introduced a statutory requirement for a chief privacy officer.[11]

Notable State Legislative Proposals

The speed, scope, and diversity of state legislative response to the issue of student data privacy has been remarkable. At the same time, the issue is complex and requires the careful balancing of:

- parents' desire to ensure the safety and welfare of their children;
- the capacity of states and districts to navigate technical privacy and security issues; and,
- the need for innovative practices to improve educational outcomes and achievement.

Legislators in some states have been challenged to strike the right balance among these factors in their proposals, sometimes with unintended consequences for parents, school districts, and technology providers. For instance, a number of notable state legislative proposals have been advanced that would place new and significant burdens on parents that would not necessarily result in heightened privacy protections for their children, including:

- Blanket requirements that each instance of a student data disclosure to third-parties – including the federal government, companies, and non-profits – require the advanced written consent of the parent or eligible student whether or not a student can be personally identified or that information would otherwise be considered directory information;
- Blanket requirements that all student data be deleted or destroyed by a school once that student leaves the school, which would restrict the ability of schools to provide transcripts to postsecondary education institutions or employers or to assess program effectiveness over time;
- Suggestions that parents may need to petition not just their school district, but other parties – such as the state and multiple third-party vendors – to review their student's education record and seek corrections, if errors are suspected.

Indeed, while the intent of provisions such as these is to empower parents to ensure the safety and welfare of their children, these provisions would disrupt the education services parents expect of their schools and dramatically increase the burden on parents to personally manage their student's education record on a day-to-day basis. In fact, given what research has shown about parent views about student data privacy and security, these types of provisions do not appear to be what parents are seeking.

Other notable provisions advanced in state legislatures would place significant new burdens on school districts that may not be well equipped to make the best decisions about technical privacy and security issues, including:

- Blanket prohibitions from the use of any third-party provider to be involved in the hosting, management, and use of student data; and,

- Requirements that each school district within a state independently negotiate detailed privacy and security provisions in contracts with every third-party provider that handles student data and with whom they have a relationship.

Taking different approaches, provisions such as these are intended to ensure that school districts have appropriate safeguards in place to ensure the privacy and security of student data. Unfortunately, both approaches introduce unintended consequences. For the first approach, state legislators should note that most school districts have for years routinely outsourced some of these functions to third-party vendors and – absent significant new resources and time to deploy them - no longer have the internal capacity, equipment, or expertise to bring these functions in house. Moreover, even with new resources school districts do not have the internal capacity to host, manage or use student data better than third parties who specialize in those practices. The second approach obligates every individual school district to retain legal counsel with expertise in security and privacy issues to review and negotiate contracts with each of their vendors that hosts, manages, or uses student data. In addition to the increased costs and time to negotiate potentially dozens of contracts annually, it also introduces a new liability risk for school districts given that the quality of legal advice will vary from community to community and that some online tools and services commonly used in schools today are offered for free and delivered absent formal contracts. A more effective approach to ensuring the adequacy of the security and privacy practices of providers working with school districts (and less burdensome to school districts, most of whom lack this capacity) would be to regulate them directly via statute.

Finally, some notable state legislative proposals would serve to discourage the development and use of innovative tools and services with the promise to dramatically improve the educational outcomes and achievement of students. For instance, some proposals have introduced:

- Requirements that vendors must be physically located within a state to provide services related to the collection, management or use of student data;
- Blanket prohibitions against using personally identifiable information for 'commercial' purposes, which – if not further defined in statute – may restrict the ability of technology and software providers to offer personalized or adaptive learning products to schools or to improve the quality of their offerings over time; and
- Requirements that vendors respond to individual parents requests to review and correct the education records of their students in situations where a vendor's relationship is with a school district, which has contracted for the provision of those services.

Provisions such as these are primarily designed to ensure that technology companies maintain control over student records and only collect and use personally identifiable data about students to provide educational services. A few issues arise with provisions such as these, however. First, geographic requirements are largely irrelevant in today's highly networked world, as the primary threats to privacy and security are not related to physical access to off-site data centers. Second, while it is critically important to establish the limits on what third-party vendors may do with the student data they collect, host, manage or use, it is

important that any new restrictions do not unintentionally hamper or prohibit the use of innovations designed to improve student outcomes and achievement via personalized or adaptive approaches to learning. Finally, while a parent's right to inspect the education records of their child must be maintained, most third-party vendors are neither equipped nor staffed to respond to requests from individual parents, which would also necessarily entail the need for vendors to verify parent identities before records could be released. Such records requests are better directed to and managed directly by school districts, with cooperation from third-party vendors, as appropriate.

CONSIDERATIONS FOR POLICYMAKERS

Nearly 40 years ago, the U.S. Department of Health, Education and Welfare issued a seminal report that was the first to articulate a comprehensive framework for how to ensure that data collections about individuals could be both fair and provide sufficient and enforceable assurances of privacy protection. Since that time, these principles have been refined and broadly adopted within the U.S. and across the world in both the public and private sectors. Known as the 'Fair Information Practice Principles' or FIPPs, this framework consists of five widely accepted principles, including: notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress.[12]

In 2014, the Foundation for Excellence in Education – building upon FIPPs and extending its framework to K-12 education – released a set of fundamental data privacy principles to guide states' review of the complex issues, laws and regulations surrounding student data privacy. ExcelinEd's student data privacy principles are:

1. *Value of data*: Student educational data is crucial for improving student outcomes and fostering an environment of personalized learning that will benefit every student.
2. *Openness*: Schools should communicate clearly with parents about how student data is collected, stored, used and shared.
3. *Limited Collection*: Schools should not collect any information beyond what is necessary for student learning and student success.
4. *Limited Use*: Students and parents need to trust that student data is protected and used solely for the purpose of improving student learning.
5. *Accurate and Accessible*: Schools must ensure that student data is accurate, up to date, and readily available to parents and students.
6. *Security*: Schools and states should clarify who is responsible for ensuring student data is protected and secure, and implement policies, systems, and procedures as necessary to ensure security.
7. *Accountability*: Schools and State Education Agencies (SEAs) should conduct compliance audits, perform related oversight and provide remedies to parents for privacy, security breaches or other misuse of student data.

From these principles and a comprehensive review of state legislative proposals, ExcelinEd developed and in 2015 updated the *Student Data Privacy, Accessibility and Transparency Act*, which is a model policy designed to provide the most comprehensive protections presently available in state law to ensure student data is used responsibly.[13] This model policy was a starting point for legislators in Georgia in what became Senate Bill 89 that was passed into law unanimously in both chambers and signed by Governor Nathan Deal. The legislation was unique in comparison to other recently enacted student data privacy laws in that it addresses

all “three legs of the stool” – data collected by government, data collected by vendors, and parental access to their own child’s data.

In addition to comprehensive and updated definitions of important terms and legislative intent, the model policy is comprised of five key sections, which together update, extend, and enhance existing federal privacy protections and as a whole directly address each of the internationally recognized FIPPs. The five key sections include – Chief Privacy Officer, Transparency/Governance/Security, Limitations on Collection and Disclosure, Company Practices, and Parental Rights – and are each described in more detail below.

Alignment of ExcelinEd Model Student Data Privacy Policy and Fair Information Practice Principles (FIPPs).

ExcelinEd Model Bill: Key Sections	Fair Information Practice Principles (FIPPs)				
	Notice/ awareness	Choice/ consent	Access/ participation	Integrity/ security	Enforcement/ redress
Chief Privacy Officer				X	X
Transparency/ Governance/ Security	X			X	X
Limitations on Collection and Disclosure	X				
Company Practices	X	X		X	
Parental Rights	X		X	X	X

Chief Privacy Officer

Aligned to Fair Information Practice Principles:

- Integrity/security
- Enforcement/redress

Education is one of the last sectors to recognize the importance of vesting primary responsibility for issues of data privacy and security in the role of a Chief Privacy Officer (CPO). The *Student Data Privacy, Accessibility and Transparency Act* envisions a CPO within the state education agency (SEA) with key responsibilities to:

- establish SEA-wide policies to assure student data privacy protections, including that the state student data system is managed in full compliance with all federal and state statutes and regulations;
- evaluate legislative and regulatory proposals involving the collection, use or disclosure of student data by the SEA, including conducting privacy impact assessments of proposals in consultation with other agencies and legal entities within the state, as necessary and appropriate;
- prepare a report annually on activities of the SEA that affect privacy, including complaints of privacy violations, internal controls, and other matters;
- establish and operate a process to ensure potential privacy violations are properly reported, investigated, and mitigated, as appropriate;
- establish and operate a process for parents to file complaints of privacy violations or inability to access education records from the responsible local education agency;
- work with other officials to engage stakeholders in issues of data quality, usefulness, openness, and privacy; and
- provide training, guidance, technical assistance, and outreach to build a culture of privacy protection, data security and data practice transparency among all state and local governmental education agencies.

The role of the Chief Privacy Officer is instrumental in ensuring that there are practices in place aligned to FIPPs at the state and local level to ensure data integrity and security, as well as for establishing a process for enforcement and redress of privacy violations.

Transparency/Governance/Security

Aligned to Fair Information Practice Principles:

- Notice/awareness
- Integrity/security
- Enforcement/redress

The *Student Data Privacy, Accessibility and Transparency Act* requires a state to:

- create, maintain and make publicly available a comprehensive inventory and dictionary of personally identifiable student data in the state data system, including the purpose for its collection;
- create and enact policies to ensure that the state data system is in compliance with all federal and state privacy statutes and regulations;
- limit access to and disclosures from the state data system except for expressly authorized purposes;

- develop a detailed physical, technical and administrative data security plan for the state data system, including guidance for local education agencies consistent with that of the state system;
- make public disclosures of proposals to expand the inclusion of personally identifiable student data in the state data system in advance of doing so on at least an annual basis; and
- develop policies and procedures to notify students and parents of their student privacy rights under federal and state law on an annual basis.

Limitations on Collection and Disclosure

Aligned to Fair Information Practice Principles:
- Notice/awareness

The *Student Data Privacy, Accessibility and Transparency Act* establishes important limits on the collection and disclosure of sensitive information about students, unless otherwise required by law or cases of health or safety emergencies. For instance, it would generally be illegal for anyone under the Act to collect data on political affiliation, voting history, income, or religious affiliation or beliefs of any student or family member. Moreover, the Act generally prohibits school districts from disclosing to the state sensitive personally identifiable information contained in juvenile delinquency records, criminal records, and medical and health records, as well as student biometric information.

Company Practices

Aligned to Fair Information Practice Principles:
- Notice/awareness
- Choice/consent
- Integrity/security

Under the ExcelinEd model policy, extensive protections are enacted to limit the types of practices companies can engage in without explicit consent from parents or eligible students, to limit disclosures of personally identifiable student data, and to ensure that companies have in place adequate privacy and security controls for the hosting, collection, management, authorized disclosure, and use of student data. For instance, under the Act, companies would be prohibited from engaging in:

- targeted advertising;

- amassing profiles of students except in furtherance of K-12 school purposes; or
- selling a student's data.

Furthermore, companies that collect personally identifiable student data would be required to implement and maintain reasonable privacy and security procedures and practices, as well as to permanently delete a student's data within a reasonable timeframe upon request of the school or local education agency.

Importantly, the Act explicitly describes and allows specific types of services and uses of data in support of personalized and adaptive learning that a company may engage in for K-12 purposes and to further student success.

Parental Rights

Aligned to Fair Information Practice Principles:
- Notice/awareness
- Access/participation
- Integrity/security
- Enforcement/redress

Parental rights to review, inspect, and seek corrections of errors in their student's education records granted by FERPA are maintained and enhanced under the *Student Data Privacy, Accessibility and Transparency Act*.

The state would be obligated under the Act to support local education agencies in fulfilling their responsibilities to:

- annually notify parents of their right to request student information,
- ensure security when providing this information to parents,
- provide guidance and best practices to local education agencies to disclose student data only to authorized individuals,
- produce education records for parents in a timely manner, and
- implement systems to allow parents to view online, download, and transmit data specific to their child's record.

For parents who have a complaint about a possible privacy violation that are not able to be resolved by inquiries the local or state education agency, the state also is obligated to create a process for parents to appeal to the state's Chief Privacy Officer. The CPO is empowered to investigate the allegations, publicly report on the outcomes, and – in cases where there is a violation of federal law – to refer the case to the appropriate authorities.

BUILDING TRUST, SPURRING INNOVATION: BEYOND LEGISLATION

While new legislation may be considered in some states to assure that procedures to protect the privacy and security of information collected about students in school are up to date, there are many actions that stakeholders can take in the absence of legislation to begin to address the issue in productive ways. In most cases, there are not legislative restrictions facing states, school districts or companies that would keep them from implementing policies and practices consistent with FIPPs – and based on surveys of parents – these actions would be warmly welcomed, even if alone they are insufficient to fully address existing concerns.

FOR FURTHER INFORMATION: ORGANIZATIONS WITH STUDENT DATA PRIVACY RESOURCES

Several leading organizations have produced resources for policymakers, school and industry leaders, and parents interested in learning more about how to best address the issues associated with student data privacy. They include:

Privacy Technical Assistance Center (PTAC) was established by the U.S. Department of Education as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. For resources and service offerings, see: http://ptac.ed.gov/

Data Quality Campaign (DQC) is a national, nonprofit advocacy organization focused on empowering educators, parents, and policymakers with quality information to make decisions that ensure students achieve their best. Extensive education privacy, security and confidentiality resources can be found online at: http://dataqualitycampaign.org/action-issues/privacy-security-confidentiality/

Consortium for School Networking (CoSN) is the national professional association for school district technology leaders. For information about CoSN's "Protecting Privacy in Connected Learning" initiative, visit: http://cosn.org/focus-areas/leadership-vision/protecting-privacy

Future of Privacy Forum (FPF) is a Washington, DC based think tank that seeks to advance responsible data practices. FPF student data privacy resources can be found online at: http://www.futureofprivacy.org/issues/student-privacy/

National Association of State Boards of Education (NASBE) is the national professional association for State Boards of Education. NASBE education data privacy resources can be found online at: http://www.nasbe.org/project/education-data-privacy/

Roles for State Education Agencies

State education agencies have an important role to play in building trust about student data use and should take the opportunity to lead the dialogue about privacy and security practices within the state. In so doing, SEAs should not delay enacting polices designed to enhance transparency, data governance, and security practices, especially with respect to the state data system.

Given that increased transparency is among the best strategies to pre-empt or address concerns about privacy, if they are not already doing so, states should publish what personally identifiable student data is collected and disclosed by the state, why it is collected, and under what authority. Moreover, states should put in place a regular process to make updates to what personally identifiable data is collected and disclosed by the state in an attempt to limit the collection of data unnecessary for educational purposes and allow for public review.

Additionally, it is critical that SEAs create governance processes and rules to vest authority for privacy and security issues in specific individuals or offices and to ensure that those with this responsibility have the authority to:

- ensure compliance with existing federal and state laws,
- authorize changes to student data collections and privacy and security practices, upon appropriate approvals,
- initiate trainings and awareness building within the SEA to help build a culture of privacy and security around

EXCELINED STUDENT DATA PRIVACY RESOURCES

ExcelinEd is actively providing support to state policymakers as they work to modernize outdated laws and respond to the concerns of parents by advancing comprehensive, balanced student data privacy protections. To assist states, ExcelinEd has recently developed:

- A framework of seven fundamental student data privacy principles as a resource for states to think about the complex issues, laws and regulations surrounding student data privacy.
- The Student Data Privacy, Accessibility and Transparency Act, which is a model policy designed to provide protections to ensure student data is used responsibly, by addressing data collected by the government, data collected by vendors and parental access to their child's data.
- Building a Trusted Environment: A Snapshot of State Laws on Student Data Use, Privacy and Security
- An online course "Data Privacy? Get Schooled.'' that discusses the value of data and offers recommendations for safeguarding student data while using it to improve student success.
- A communications toolkit with model resources school districts can adapt to communicate with parents and other stakeholders;
- A model contract checklist for key components to include in agreements with vendors that host, manage, or use student data;
- A model parent notification communications regarding the privacy and security of student records, including the delineation of parent rights under law; and
- Model training resources for teachers, which include tips on appropriate approaches and strategies to protect student data.

To access these resources, please visit: http://excelined.org/student-data-privacy/

student data, and
- coordinate and communicate with other stakeholders in the state about privacy and security issues.

With the agency, SEAs should review their physical, technical and administrative data security procedures and processes on at least an annual basis and update them to ensure compliance with best practices. Access to student data should only be granted to those with a specific need for the data and should only be disclosed for purposes that have been expressly defined. Moreover, a record of access to and disclosures of student data should be maintained for audit purposes.

Finally, states have a valuable role to play in building the capacity of school districts to manage the privacy and security of student data. Local education agencies would benefit from model guidance and best practice information, as well as up to date information on federal and state privacy legislation and regulation. ExcelinEd offers a number of resources that states could adapt and employ to engage districts in this regard, including:

- Model contract checklist for key components to include in agreements with vendors that host, manage, or use student data;
- Model parent notification communications regarding the privacy and security of student records, including the delineation of parent rights under law; and
- Model training resources for teachers, which include tips on appropriate approaches and strategies to protect student data.

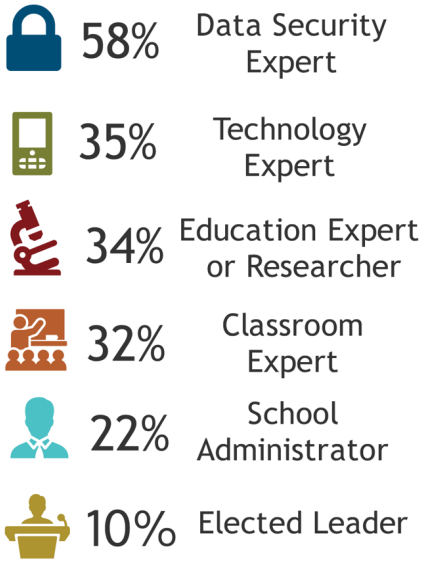
Roles for School Districts

School districts have the primary responsibility for ensuring the safety and welfare of their students, including with regard to the privacy of data about students. As such, school districts should strive to enhance transparency and communication practices about the collection and handling of student data, evaluate and enhance their own security and privacy practices, and ensure that teachers, administrators, and other staff have the training and tools they need to carry out their privacy and security responsibilities.

WHO DO PARENTS TRUST ON STUDENT DATA PRIVACY ISSUES?

Unlike many other issues related to education policy and practice, where direct classroom experience is held in the highest regard by parents seeking advice on an issue, parents reported that they were most likely to trust someone to address student data privacy concerns if they had expertise in data security issues, followed by those with technology experience and then those with a background as an education expert or researcher.

The following is how parents ranked the trustworthiness of individuals with different experience:



An individual or office within the district should be empowered to be responsible for issues of student data privacy and security, including monitoring compliance with federal and state laws, responding to requests and questions from parents and vendors, offering training and support to teachers, administrators and other district staff, and communicating to stakeholders. This individual or office should prepare annual notifications to parents of their rights under law to review student records and establish procedures to ensure that parent rights are upheld in a timely and responsive manner.

School districts should be transparent with their local communities about which vendors they use, what student data is shared with them, and the privacy and security provisions in place in contracts with vendors to ensure student data privacy.

In addition to seeking support from privacy experts at state education agencies and the U.S. Department of Education's Privacy Technical Assistance Center (PTAC), school districts should strongly consider working in partnership with other school districts and/or regional service state education agencies within the state to develop and refine model processes and communications (such as those developed by ExcelinEd).

Finally, school districts should incorporate information about privacy into any ongoing internet safety and cyber-bullying curricula used with students. This is especially important in that some students today may overshare personal information online in ways that could be embarrassing, if not also detrimental to their future.

COMMON QUESTIONS PARENTS HAVE ABOUT STUDENT DATA PRIVACY

In an effort to garner more specific information about the types of questions and concerns parents may have about the privacy of student data, ExcelinEd's 2015 national public opinion research study conducted by Echelon Insights asked parents about questions they may have for school districts about the issue. Parents reported that their most important questions included:

1. *Who has access to this student learning data?*
2. *What laws are in place to protect student data privacy?*
3. *How is the data being protected and kept secure?*
4. *What type of data is being collected about student learning?*
5. *What can companies use the data for?*

Parents' priorities clearly seem to be directed at understanding the boundaries and protections in place to safeguard information collected about their children, especially when that information may be shared with those beyond their own school district. Schools should be prepared to answer these and related parent questions, including by proactively communicating related information to parents in writing and in face-to-face meetings.

Roles for Parents

As they do with other aspects of their children's education, parents have a critical and welcome role to play in building a culture of privacy and trust in education. At a minimum, parents should be encouraged to read and review official notifications sent to them about the collection and disclosure of information about students, paying special attention to the rights

that they are afforded to opt out of certain data collections and to review the education records of their children.

In addition, parents should be invited to engage in dialogue with their school and school district officials about the district's data privacy practices, including by asking questions such as:

- What products or services are used by the district that involve the collection or sharing of student data?
- What types of information is shared with the providers of these services?
- What privacy and security protections are in place for student data?
- What training does staff in schools get to ensure they understand their responsibilities for ensuring student data privacy?

Just as important, parents also have an important role to play in concert with schools to helping to teach their children to be safe and responsible in sharing personal information online, on social media, and via apps on tablets and smartphones. No matter what protections may be in place in schools, some students tend to overshare online. It is critical, therefore, for students to be taught how to be responsible for their own behavior.

Roles for Companies

While companies also have a stake in legislative proposals to safeguard student data privacy – and must be in compliance with current federal and state laws and regulations – those that host, collect, manage or use student data have a critical role to play in building parent and educator trust. There are many productive and welcome steps that companies can take outside of participating in the legislative process, including improving communications and data handling practices.

For instance, companies can ensure that they clearly communicate what their tool or service does for K-12 schools and students, what types of personally identifiable student data they collect and how they use it, and their privacy and security policies and practices. Importantly, these communications must be understandable to non-technical audiences, easily accessible online, and written in plain language.

At the same time, companies should evaluate their internal procedures and processes to minimize the collection of personally identifiable student data and ensure they are keeping it only for as long as strictly necessary for the provision of educational services.

Finally, companies that have not already signed the Student Privacy Pledge developed by the Future of Privacy Forum and the Software & Information Industry Association should consider doing so as a way to help reassure customers and parents of their good faith commitment to addressing student data privacy issues.[14]

CONCLUSION

There can be little argument that ensuring the privacy and security of student data is a critical issue that needs to be addressed in the move to personalized education. However, given the complexity of the issue and its relationship to the implementation of other important education policies, it is important for policymakers to ensure that in responding to this issue that they adequately address parents' privacy concerns without unintentionally undermining schools' ability to help prepare students for further education, life, work, and citizenship in an increasingly technology-driven world. The good news is that while the issue is complex, there is research available to shed light on the context for the privacy of student data as an issue and on parental concerns more specifically. In addition, organizations such as ExcelinEd have created model policies and other valuable resources for policymakers and school leaders to build upon. Working together, we can help schools ensure the safety and welfare of students in a digital age.

NOTES

[1] School responses to issues of internet safety have been supported by the work of many, including experts, advocates, and policymakers. For example, the passage in 2000 of the *Children's Internet Protection Act* established baseline internet safety regulations for students in schools and libraries that participate in the E-rate program. For further information, see: https://www.fcc.gov/guides/childrens-internet-protection-act

[2] Perhaps the most significant breach of student privacy to date in K-12 education was perpetrated by a Pennsylvania school district during the 2009-10 school year, which deployed laptops to students with tracking software that was activated remotely by district employees in questionable circumstances. The district was sued over the invasion of student privacy and has spent more than $1.2 million in fees and costs associated with settlements paid to student plaintiffs. For more, see: Chloe Albanesius, "Pa. School Sued (Again) Over Webcam Spying," PC Magazine, June 8, 2011. Available online at: http://www.pcmag.com/article2/0,2817,2386599,00.asp

[3] Natsha Singer, "Data Security Gaps in an Industry Student Privacy Pledge," *New York Times*, February 11, 2015. Available online at: http://bits.blogs.nytimes.com/2015/02/11/data-security-gaps-in-an-industry-student-privacy-pledge/?_r=0

[4] "Testing, testing: A review session on COPPA and schools," Federal Trade Commission, accessed August 6, 2015, https://www.ftc.gov/news-events/blogs/business-blog/2015/01/testing-testing-review-session-coppa-schools

[5] RAND Corporation and the Bill & Melinda Gates Foundation, *Early Progress: Interim Research on Personalized Learning* (Seattle, WA: Bill & Melinda Gates Foundation, 2014), http://collegeready.gatesfoundation.org/learning/early-progress-interim-report-on-personalized-learning/

[6] For a definition of blended learning and related information, see resources created by the Clayton Christensen Institute for Disruptive Innovation at http://www.christenseninstitute.org/blended-learning/

[7] Evergreen Education Group and Clayton Christensen Institute for Disruptive Innovation, *Proof Points: Blended Learning Success in School Districts - Horry County Schools (Conway, South Carolina)* (Durango: CO: Evergreen Education Group, 2015), http://www.christenseninstitute.org/wp-content/uploads/2015/06/Horry-County-Schools.pdf

[8] Evergreen Education Group and Clayton Christensen Institute for Disruptive Innovation, *Proof Points: Blended Learning Success in School Districts - Spokane Public Schools (Spokane, Washington)* (Durango: CO: Evergreen Education Group, 2015),

http://www.christenseninstitute.org/wp-content/uploads/2015/04/Spokane-Public-Schools.pdf

[9] Evergreen Education Group and Clayton Christensen Institute for Disruptive Innovation, *Proof Points: Blended Learning Success in School Districts - District of Columbia Public Schools (Washington, DC)* (Durango: CO: Evergreen Education Group, 2015), http://www.christenseninstitute.org/wp-content/uploads/2015/05/DCPS.pdf

[10] For parents uncomfortable with their school's data sharing practices, this may include the ability to opt out of having their child complete certain tests and assignments using education technology tools in order to protect their child's data from being shared with the companies that run these tools. For an extended discussion of issues related to parent consent and opt out in the K-12 context, see: Jules Polonetsky and Joseph Jerome, *Student Data: Trust, Transparency, and the Role of Consent* (Washington, DC: Future of Privacy Forum, 2014), http://www.futureofprivacy.org/wp-content/uploads/FPF_Education_Consent_StudentData_Oct2014.pdf

[11] Foundation for Excellence in Education and EducationCounsel, *Building a Trusted Environment: A Snapshot of State Laws on Student Data Use, Privacy and Security* (Tallahassee, FL: Foundation for Excellence in Education, 2015), http://excelined.org/studentdataprivacysnapshot/

[12] Federal Trade Commission, *Privacy Online: A Report to Congress* (1988), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

[13] Foundation for Excellence in Education, *Student Data Privacy, Accessibility, and Transparency Act Model Policy* (Tallahassee, FL: Foundation for Excellence in Education, 2015), can be accessed through http://excelined.org/student-data-privacy

[14] Information about the Student Privacy Pledge can be found online at: http://studentprivacypledge.org/

Stay Connected

EXCELINED.ORG

FACEBOOK.COM/EXCELINED

@EXCELINED