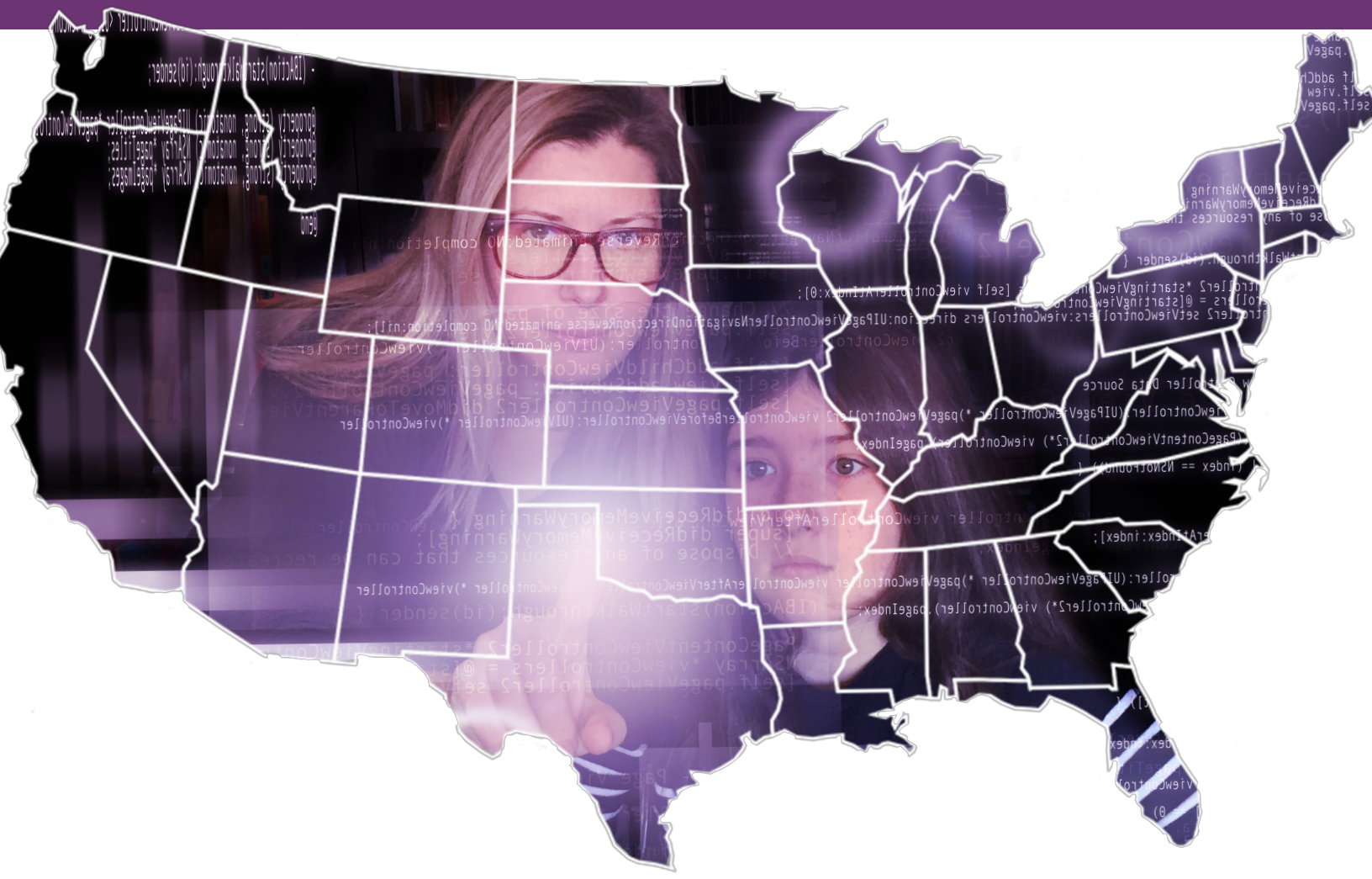
THE STATE STUDENT PRIVACY REPORT CARD

GRADING THE STATES ON PROTECTING STUDENT DATA PRIVACY



JANUARY 2019

PARENT COALITION FOR STUDENT PRIVACY

THE NETWORK FOR PUBLIC EDUCATION

ACKNOWLEDGMENTS

Rachael Stickland, Co-Chair of the Parent Coalition for Student Privacy, was the primary author of this report. Leonie Haimson, Executive Director of Class Size Matters and Co-Chair of the Parent Coalition for Student Privacy, also contributed to the report's writing and editing.

The report would also not have been possible without the effort and commitment of those listed below:

The Board of Directors of the Network for Public Education (NPE) and Class Size Matters, with special thanks to Diane Ravitch, President of NPE. Carol Burris and Darcie Cimarusti of NPE who provided technical oversight, writing and editing assistance.

And especially, all the individual donors and foundations that support our work.

About the Network for Public Education

The Network for Public Education (NPE) is an advocacy group whose mission is to preserve, promote, improve and strengthen public schools for both current and future generations of students. The goal of NPE is to connect all those who are passionate about our schools – students, parents, teachers and citizens. We share information and research on vital issues that concern the future of public education at a time when it is under attack. For more information, please visit our website at www.networkforpubliceducation.org.

About the Parent Coalition for Student Privacy

The Parent Coalition for Student Privacy (PCSP) is a project of Class Size Matters. Established in 2014, PCSP is national alliance of parents and advocates with the goal promoting strong local, state, and national policies and practices to protect and secure personal student data. For more information, please visit our website at www.studentprivacymatters.org.

TABLE OF CONTENTS

Figures

WHY THIS REPORT IS NEEDED

In 1974, Congress passed legislation known as the *Family Educational Rights and Privacy Act* or FERPA, in response to "the growing evidence of the abuse of student records across the nation."[1] The law was written to protect the confidentiality of information held in a student's records, which at the time were usually stored in a locked filing cabinet in the principal's office and accessed primarily by school employees who needed it to perform their professional duties.

With the introduction of technology in schools, education has changed dramatically since FERPA was enacted forty-five years ago. Digital record-keeping has replaced traditional paper files, classroom assignments and assessments are often delivered online via laptops or tablets, teachers use social media platforms, websites and "free" apps in class, and many operational functions historically performed by schools are now outsourced remotely to contractors. As a result, students generate enormous amounts of sensitive electronic data about themselves every day, not all of which is clearly protected by federal law. Compounding the problem, FERPA has been weakened numerous times over the years through regulatory changes, making it easier for schools to collect and share this data with large private corporations, including Silicon Valley giants like Google, Facebook, and Microsoft, as well as thousands of smaller ed tech companies, many of them start-ups who offer their wares for free to schools in exchange for access to student data.

These issues came into focus in 2013 when the Bill & Melinda Gates Foundation sparked a national controversy with its proposed $100 million data warehouse project called inBloom, Inc. Originally piloted in nine states across the country, inBloom was developed to standardize student data collection, store it in the cloud, and make it available to for-profit vendors to develop and market their products and services, without parental knowledge or consent. Parents – and even some school officials – in affected districts were shocked to learn that FERPA and other related federal laws had been weakened to allow for this non-consensual use and disclosure of student data.

inBloom shut its doors in 2014 due to significant parental backlash, but not before igniting fierce concerns about student privacy. As a result, state legislatures across the country began introducing bills to close the loopholes and gaps in FERPA and other federal laws. Since 2013, over 120 student privacy-related laws in at least 40 states have been passed, creating a confusing patchwork of statutes.

1 121 Cong. Rec. 13990 (daily ed. May 13, 1975)

Though some organizations have tracked this legislation, what has so far been missing is a comprehensive analysis of student privacy laws that evaluates their strength in terms of transparency, parental and student rights, data security protections, and other critical issues. The Network for Public Education and the Parent Coalition for Student Privacy created this report card to provide a snapshot of the legal progress made by the fifty states and the District of Columbia to protect students' privacy since 2013.

Our hope is that this report card will be used by parents and elected officials to better understand how their state's student privacy protections compare to others, and how they could be improved.

Disclaimer

While the goal of this report is to provide a glance of the protections in state student privacy laws, our analysis should not be used in place of legal advice from an attorney. For questions on how state, or federal and local laws and policies may apply to your particular situation, you should seek the advice of a licensed attorney by contacting your local bar association's referral service.

Report Card with State Grades

No states earned an "A" overall, as no state sufficiently protects student privacy in our estimation to the degree necessary. Colorado earned the highest weighted average grade of "B." Three states – New York, Tennessee and New Hampshire– received the second highest weighted average grade of "B-." Except for New York, all other states earning a "B" or "B- "enacted more than one student privacy law.

Every state received points and grades on each of the following seven categories: Parties Covered and Regulated; Transparency; Parental and Student Rights; Limitations on Commercial Use of Data; Data Security Requirements; Oversight, Enforcement, and Penalties for Violations; and Other Provisions.

State grades were assigned using the Grade Point Average scale in **Figure 1**.

FIGURE 1 - STATE GRADE SCALE

Grade	GPA Range	# of States
A+	(3.67)-(4.0)	0
A	(3.34)-(3.66)	0
A-	(3.01)-(3.33)	0
B+	(2.67)-(3.0)	0
B	(2.34)-(2.66)	1
B-	(2.01)-(2.33)	3
C+	(1.67)-(2.0)	8
C	(1.34)-(1.66)	6
C-	(1.01)-1.33)	5
D+	(0.67)-(1.0)	12
D	(0.34)-(0.66)	2
D-	(0.01)-(0.33)	3
F	0	11

States are ranked by their overall grades from highest to lowest below, as well as their GPA, points and number of student privacy laws in **Figure 2**. You can also see the full map of grades at a glance on the websites of the Network for Public Education and the Parent Coalition for Student Privacy.

Figure 3 is a chart showing each state's grade in each of the seven categories described.

FIGURE 2 - 2019 STATE OVERAL GRADES HIGH TO LOW

State Name	State Grade	Weighted Average GPA	Total Points	# Laws
Colorado	B	2.37	49.0	2
New York	B -	2.32	40.0	1
Tennessee	B -	2.30	43.5	4
New Hampshire	B -	2.12	44.5	12
Nevada	C+	1.95	32.5	2
Georgia	C+	1.93	32.5	1
North Carolina	C+	1.92	29.5	2
Virginia	C+	1.83	29.0	12
Illinois	C+	1.82	33.0	3
Missouri	C+	1.82	27.5	1
Connecticut	C+	1.80	34.5	4
Kansas	C+	1.70	26.5	2
Utah	C	1.58	31.5	6
Delaware	C	1.58	27.5	1
West Virginia	C	1.55	29.5	2
Idaho	C	1.55	26.5	1
California	C	1.50	30.0	4
Arizona	C	1.35	21.0	2
Maine	C-	1.18	19.5	5
Arkansas	C-	1.13	15.0	3
Indiana	C-	1.12	18.5	1
Oregon	C-	1.12	15.0	2
Louisiana	C-	1.03	22.5	4
Washington	D+	1.00	9.5	1
Hawaii	D+	0.98	12.0	1
Kentucky	D+	0.98	10.0	1
Rhode Island	D+	0.97	12.0	1
Nebraska	D+	0.95	11.0	1
DC	D+	0.92	13.5	1
Texas	D+	0.88	9.5	2
Maryland	D+	0.78	10.5	3
Michigan	D+	0.75	15.0	2
Oklahoma	D+	0.75	13.0	1
Florida	D+	0.75	12.5	1
Iowa	D+	0.75	7.0	1
Wyoming	D	0.62	12.0	2
South Dakota	D	0.54	9.0	1
North Dakota	D-	0.33	7.0	1
Pennsylvania	D-	0.17	4.5	1
Ohio	D-	0.07	1.0	1
Alabama	F	0.00	0.0	0
Alaska	F	0.00	0.0	0
Massachusetts	F	0.00	0.0	0
Minnesota	F	0.00	0.0	0
Mississippi	F	0.00	0.0	0
Montana	F	0.00	0.0	0
New Jersey	F	0.00	0.0	0
New Mexico	F	0.00	0.0	0
South Carolina	F	0.00	0.0	0
Vermont	F	0.00	0.0	0
Wisconsin	F	0.00	0.0	0

FIGURE 3 - STATE GRADES BY CATEGORY

State Name	Parties Covered & Regulated	Transparency	Parental & Student Rights	Commercial Uses	Data Security	Oversight & Enforcement	Other Provisions	Overall Grade
Alabama	F	F	F	F	F	F	F	F
Alaska	F	F	F	F	F	F	F	F
Arizona	C-	F	C	C	D	C	F	C
Arkansas	C	F	C-	C	D	D	F	C-
California	C+	D+	B-	C	D	D	F	C
Colorado	C+	B+	B+	B	B-	F	C	B
Connecticut	C+	B+	C	C	C	C-	F	C+
Delaware	C	F	C	C	C-	C	D-	C
DC	D+	F	D+	D+	C	F	F	D+
Florida	D+	F	C-	F	F	C-	D-	D+
Georgia	C	C	B-	C	C+	D	F	C+
Hawaii	D	F	C	C	D	F	F	D+
Idaho	C-	C	F	D+	C+	B-	D+	C
Illinois	B	F	C	C	D	B+	D+	C+
Indiana	C-	D	C-	F	C-	C-	F	C-
Iowa	D	F	D	C	D	F	F	D+
Kansas	C-	D+	C+	C	C-	C-	F	C+
Kentucky	D	D	D	B-	F	F	F	D+
Louisiana	C-	B	D	F	C-	C-	C+	C-
Maine	C	F	C	C	D	F	D-	C-
Maryland	C-	F	D+	D+	D	F	F	D+
Massachusetts	F	F	F	F	F	F	F	F
Michigan	C	C-	C	F	D	F	F	D+
Minnesota	F	F	F	F	F	F	F	F
Mississippi	F	F	F	F	F	F	F	F
Missouri	D+	C	C-	C	C	C	D	C+
Montana	F	F	F	F	F	F	F	F
Nebraska	D	F	C	C	D	F	F	D+
Nevada	C	B-	C-	C	C+	C	F	C+
New Hampshire	B	C+	B+	B-	D-	F	B+	B -
New Jersey	F	F	F	F	F	F	F	F
New Mexico	F	F	F	F	F	F	F	F
New York	C	C+	C-	A-	B+	D	D	B -
North Carolina	D+	C-	B-	C	B-	C-	F	C+
North Dakota	D+	F	F	F	C-	F	F	D-
Ohio	D-	F	F	F	F	F	F	D-
Oklahoma	D	C	F	F	C	F	D	D+
Oregon	C	F	D+	C	D	D	F	C-
Pennsylvania	D+	F	F	F	F	F	D-	D-
Rhode Island	D	D	F	C	F	C-	D+	D+
South Carolina	F	F	F	F	F	F	F	F
South Dakota	D	F	C-	F	D-	F	F	D
Tennessee	C+	C	B	B-	B-	C-	C+	B -
Texas	D+	F	D+	C	D	F	F	D+
Utah	C	C+	C-	D	C+	C	D-	C
Vermont	F	F	F	F	F	F	F	F
Virginia	B-	D	C	B-	C	D	D-	C+
Washington	D	D	D+	C	D	F	F	D+
West Virginia	C-	C+	C+	F	C+	D	D+	C
Wisconsin	F	F	F	F	F	F	F	F
Wyoming	C-	F	F	F	C-	D	D	D

Methodology

We used seven categories to evaluate each state's student privacy laws. Five categories are aligned with the core principles that the Parent Coalition for Student Privacy developed in 2015[2]: 1) Transparency; 2) Parental and Student Rights; 3) Limitations on Commercial Use of Data; 4) Data Security Requirements, and 5) Oversight, Enforcement, and Penalties for Violations.

Two additional categories were added: 1) Parties Covered and Regulated; and 2) Other, a catch-all for provisions of state laws that did not fit into any of the above categories. Each category was given a weight depending on how important we believed it was to the overall goal of protecting student privacy, as listed in **Figure 4** below.

FIGURE 4 - POINTS POSSIBLE AND CATEGORY WEIGHT

	Category	Points Possible	Percentage
1	Parties Covered and Regulated	16	10%
2	Transparency	16	15%
3	Parental and Student Rights	26	20%
4	Limitations on Commercial Use of Data	14	20%
5	Data Security Requirements	12	15%
6	Oversight, Enforcement, and Penalties for Violations	12	15%
7	Other Provisions	+/-4	5%
	Total	**100**	**100%**

We also catalogued each law's definition of important terms, but this category is for reference only – no points were awarded or deducted. You can find the types of terms we tracked in the Technical Appendix on page 1, as well as specific interpretations of those definitions online in our comprehensive comparison matrix of state student privacy laws that includes a link to each of these laws. Provisions targeted specifically to protect teacher data privacy were also identified in our spreadsheet. However, any points awarded for these provisions were assigned to the appropriate categories, using the same method applied to other parties covered by the law, e.g. K-12 students.

While over 120 data privacy laws have been enacted since 2013, we focused our analysis on 99 laws passed in 39 states plus the District of Columbia between 2013 and 2018 that specifically addressed student privacy and data security protections. General data security and breach notification legislation that did not explicitly apply to student data and/or laws pertaining to the use of social media by adults or individuals outside of the

[2] Five Principles to Protect Student Privacy. Parent Coalition for Student Privacy, www.studentprivacymatters.org/five-principles-to-protect-study-privacy/.

school context were not included in the report card. We included the *Illinois School Student Records Act*, first passed in the late 1970s and amended over time,[3] because the law is generally regarded as one of the stronger pieces of state student privacy legislation enacted in the post-FERPA/pre-inBloom era. The eleven states with no student privacy laws automatically received an "F."

For our analysis, we identified 30 measurable factors that guided the ratings of the seven categories. Using the best sources of information available, we devised a point scale for each factor and then evaluated each state's law(s) against these 30 factors. Points in each category were tallied, and then assigned a Grade Point Average (GPA) and a letter grade "A" to "F" based on a point scale, as described in the Technical Appendix. When a state received negative points in a specific category, points were deducted from that category's average GPA.

The seven letter grades were then weighted to create an overall GPA, which was finally converted into a total letter grade. For a state with more than one student privacy law, we used the "additive" method, considering all its laws together across categories. If none of the state's laws covered a specific category, it received zero points for that category.

A more detailed explanation of our methodology can be found in the Technical Appendix, which includes a link to a comparison matrix of all 99 state privacy laws that we graded. The matrix also links to each of the state laws directly, so that parents, advocates and concerned citizens in these states can learn about them in more detail.

Major Findings

Most state student privacy laws enacted between 2013 and 2018 fall into one of the five following groups:

1. Laws modeled after the California's 2014 law known as the *Student Online Personal Information Protection Act* (SOPIPA);[4]

2. Laws patterned after the Foundation for Excellence in Education's 2015 model bill, known as the *Student Data Privacy, Accessibility, and Transparency Act*;[5]

3. Laws that established access and security standards for statewide longitudinal data systems (SLDS),

---

[3] 105 ILCS 10/ Illinois School Student Records Act. 720 ILCS 5/ Criminal Code of 2012, www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=1006&ChapterID=17.

[4] Herold, Benjamin. " 'Landmark' Student-Data-Privacy Law Enacted in California." Education Week - Teacher Beat, 1 Oct. 2014, blogs.edweek.org/edweek/DigitalEducation/2014/09/_landmark_student-data-privacy.html.

[5] Student Data Privacy, Accessibility, and Transparency Act. The Foundation for Excellence in Education, www.excelined.org/wp-content/uploads/Student-Data-Privacy-Accessibility-and-Transparency-Act-Model-Legislation-03.2015.pdf.

while also authorizing state education departments to collect and share personal student data among several state agencies;

4. Laws that prohibit the collection or disclosure of Social Security numbers, biometric or other especially sensitive personal student information; and

5. Laws to regulate schools' access to students' social media accounts.

Twenty-three states and the District of Columbia have passed laws modeled after California's SOPIPA. Spearheaded by the organization Common Sense Media in collaboration with representatives from the tech industry, SOPIPA was widely regarded as a "landmark" law to protect student information collected by online companies offering technology services.

While SOPIPA was a good starting point, in our view the original law and weakened versions subsequently passed in some other states fell short in certain areas and could be improved. For example, the original version only prohibits companies from "knowingly" selling student data or using it to create a profile of the student for non-educational purposes. However, the sale of student data was allowed in purchases, mergers or other type of acquisitions.

The weaker versions of SOPIPA passed in several states allowed targeted advertising to students under certain circumstances, and exempted from the law companies that offer college and career readiness assessments, such as the ACT exams and the College Board's SAT. States that passed the weakened version included Arizona and Texas.

States with laws modeled after the Student Online Personal Information Protection Act (SOPIPA)

Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Georgia, Hawaii, Illinois, Iowa, Kansas, Maine, Maryland, Michigan, Nebraska, Nevada, New Hampshire, North Carolina, Oregon, Tennessee, Texas, Utah, Virginia, and Washington.

Most states that solely passed a SOPIPA-like law, and no other law to safeguard student privacy, received a weighted average grade of between "C+" to "D-" in our report card, depending on whether they passed the original or a weakened version.

Nine states modeled their legislation after the *Student Data Privacy, Accessibility, and Transparency Act*, first developed by the Foundation for Excellence in Education.[6] These laws generally require state education departments and state boards of education to increase transparency around the personal student data they collect, develop a data security plan, and provide guidance to local school districts on how to protect it. Most

[6] ibid.

On the issue of "Targeted Advertising"

While students are browsing the internet or using an online program assigned by their schools, ads for products based on their personal interests or school-related services often pop up on their screens. How their browsing data is gathered by online companies and then used for digital advertising is a complex and opaque practice that was first addressed in state privacy law with the passage of California's 2014 SOPIPA. Although it was the first state to ban operators of education websites and online services from "targeted advertising" to students, the term was never clearly defined, leaving both companies and students confused as to which ads were allowed and which were not.

Subsequent efforts by other states to enact laws modeled after SOPIPA attempted to define "targeted advertising" to mean when a company presents ads to students based on information obtained or inferred from their online behavior, usage of applications, or personal data. Most of these laws, however, provided loopholes or exceptions permitting companies to display targeted ads to students based upon their current visits to an education website (or online service), or in response to their requests for information (i.e. search queries), as long as their online activities or data were not retained to create "profiles" to market to them and/or target ads to them over time. Though we believe no company should be using students' information to market products or services, whether their demographic data such as age, gender or geolocation, or online behavior, such as the time spent on particular websites, we did award partial points to states that made at least some effort to limit this practice.

laws in this category also create a position of a Chief Privacy Officer within the state department of education or a similar post, and some limit commercial uses of student information. Oklahoma was the first state to enact this legislation in 2013, which because of its relative weakness in certain areas earned it an overall average grade of "D+."

In general, the remaining states passed laws that establish security requirements for specific data systems, or limit the date and disclosure of sensitive information, including students' social media passwords.

States with laws patterned after the Student Data Privacy, Accessibility, and Transparency Act model legislation

Colorado, Georgia, Idaho, Missouri, Nevada, North Carolina, Oklahoma, Tennessee, and West Virginia.

Components and Categories to Calculate State Grades

Parties Covered and Regulated

Our underlying assumption for this category is that the more parties, such as students or educators, whose data are legally protected, and the more entities with access to the data that are regulated, the stronger the law.

Determining which groups are protected or "covered" by state laws and which parties receiving the data had their use restricted was the first step in our evaluation process.

We used four factors to determine each state's grade in this category.

1. Categories of covered students, including pre-Kindergarten, K-12, and post-secondary or higher education;

2. Other parties whose data is covered, including teachers and principals;

3. Education agencies regulated, including the state board of education, the state department of education, local school districts, public schools, private schools, and charter schools; and

4. Private entities or third parties regulated, including vendors, contractors, sub-contractors, operators, online service providers, and researchers.

The summary of state grades for covering and regulating parties is listed in **Figure 5**.

Illinois and New Hampshire received the highest mark of "B" for protecting the data privacy of many different parties and regulating the behavior of many entities with access to the data. Other than the eleven states that received an "F" for failing to pass any privacy law at all, Ohio received the lowest grade of "D-" for not identifying any parties that would be legally protected.

FIGURE 5 - Parties Covered and Regulated Grade Summary

Grade	# States	State Names
A+	0	None
A	0	None
A-	0	None
B+	0	None
B	2	Illinois, New Hampshire
B-	1	Virginia
C+	4	California, Colorado, Connecticut, Tennessee
C	9	Arkansas, Delaware, Georgia, Maine, Michigan, Nevada, New York, Oregon, Utah
C-	8	Arizona, Idaho, Indiana, Kansas, Louisiana, Maryland, West Virginia, Wyoming
D+	7	District of Columbia, Florida, Missouri, North Carolina, North Dakota, Pennsylvania, Texas
D	8	Hawaii, Iowa, Kentucky, Nebraska, Oklahoma, Rhode Island, South Dakota, Washington
D-	1	Ohio
F	11	Alabama, Alaska, Massachusetts, Minnesota, Mississippi, Montana, New Jersey, New Mexico, South Carolina, Vermont, Wisconsin

Transparency

Parents reasonably expect that any personal information collected about their child by the school, other government agencies, or private entities will be respected and kept confidential. As such, schools and districts should be clear about their student privacy policies and practices and communicate them accurately to parents. Knowing how their children's school handles personal student information allows parents to determine whether data protections in place are adequate.

We believe that parents should be informed as to which student data is being collected by schools and districts, for what purposes, why it is being shared and with whom. When student data is disclosed to third parties, the school should require a written and signed agreement, detailing the responsibilities of each party, including how that data will be secured.

Colorado and Connecticut received the highest mark of "B+" in this category for requiring transparency in the use and disclosure of student data. Of those states with student privacy laws, Arizona, Arkansas, Delaware, District of Columbia, Florida, Hawaii, Illinois, Iowa, Maine, Maryland, Nebraska, North Dakota, Oregon, Pennsylvania, South Dakota, Texas, and Wyoming received "F"s for failing to require education agencies and private entities to be transparent about their data collection and use practices.

We used the following four factors to determine each state's grade for its data transparency practices. States received points based on:

1. The extent to which education agencies are required to identify what student data they collect, the purpose/use of each collection, and how this information is made available to parents and the public;

2. The extent to which education agencies and schools are required to execute a written agreement before sharing student data with third parties;

3. The extent to which these written agreements are made available to parents and the public; and

4. The extent to which these agreements include specific data privacy and security protections.

The summary of state grades for transparency in the collection and use of data is listed in **Figure 6**.

FIGURE 6 - Transparency Grade Summary

Grade	# States	State Names
A+	0	None
A	0	None
A-	0	None
B+	2	Colorado, Connecticut
B	1	Louisiana
B-	1	Nevada
C+	4	New Hampshire, New York, Utah, West Virginia
C	5	Georgia, Idaho, Missouri, Oklahoma, Tennessee
C-	2	Michigan, North Carolina
D+	2	California, Kansas
D	5	Indiana, Kentucky, Rhode Island, Virginia, Washington
D-	0	None
F	29	Alabama, Alaska, Arizona, Arkansas, Delaware, District of Columbia, Florida, Hawaii, Illinois, Iowa, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Montana, Nebraska, New Jersey, New Mexico, North Dakota, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Texas, Vermont, Wisconsin, Wyoming

On the Issue of "Consent"

Twenty-six states give students and parents some rights to consent to the release, use, or deletion of information. Some states allow the right to consent to specific types of disclosures or uses of student data by operators providing online products and services to schools. While we applaud these states for engaging students and parents in decision-making about their data, it is not clear that families always fully understand what it is they are consenting to.

For example, Nevada allows operators to create personal profiles of students for non-instructional purposes with the consent of an eligible student or parent. Because the law fails to describe how permission must be obtained, it is unclear whether agreeing to the Terms of Service before using an ed tech website simply by clicking the "I accept" box would suffice as "consent" – especially when the majority of users never read the fine print of such agreements.

In the District of Columbia, students over the age of thirteen or their parents can give consent to operators to "sell, rent, or trade" their information for the "purpose of providing the student with information about employment, educational scholarship, financial aid, or postsecondary educational opportunities." Arizona, Colorado, Nebraska, North Carolina, and Texas also allow eligible students, which generally means children attending K-12 public schools, to consent to the use of their data for these purposes. This issue often comes into play when students volunteer personal information to the College Board or ACT prior to their taking exams, which according to their websites, may be used to match them with colleges and scholarship opportunities. But when students check the box agreeing to sharing their information, they may have unknowingly consented to their data being sold, rented, or traded to colleges, companies or for-profit organizations that may in turn use this information to market to them, redisclose the information to yet other vendors, use the data to expand their applicant base to boost their ratings, or decide whom to accept or reject. The College Board and ACT do indeed sell access to personal student data and have been accused of engaging in many of these other activities.

Parental and Student Data Rights

Unfortunately, the U.S. Department of Education's guidance and regulations concerning the privacy of student records as delineated in FERPA has weakened over time, allowing for broader disclosure of student data to vendors, researchers and other private entities without parental notification or consent. While FERPA requires that parents can challenge and correct errors in their children's education records, and opt out of certain disclosures, they often do not have the ability to do so in the case of companies or organizations that provide various types of services to schools, whether for operational, instructional, evaluation or research purposes.

Additionally, the Department's guidance is often ambiguous as to whether data held by online vendors is even subject to regulations of the law. According to one U.S. Department of Education document, written to respond to the question, "Is Student Information Used in

Online Educational Services Protected by FERPA?", the ambiguous answer is, "It depends. Because of the diversity and variety of online educational services, there is no universal answer to this question."[7]

Without clearer guidance from the federal government, states have stepped in to fill the gap, attempting to more specifically define what rights parents and students have over their own personally identifiable information, especially when it is collected directly by online vendors used by schools.

We believe students and their parents should own their personal data and control its use and disclosure in most instances. Decisions about how their data is used and with whom it may be shared should be made only with the full knowledge of students and their parents, and if possible, with their consent – especially when it involves highly sensitive information such as children's disabilities, health, and disciplinary records.

We gave high grades to states that made meaningful attempts, both in the spirit and the letter of the law, to acknowledge that students and their parents have certain rights to make informed decisions as to how their personal data will be disclosed and/or used.

In the category of parental or student rights, we assigned grades to state laws according to the following seven factors:

1. The extent to which parents can access and correct student data collected by private entities, delete the information if it is in error or nonessential to the student's education record, and opt-out of further collection;

2. The extent to which certain sensitive student data, including Social Security numbers and biometric data, cannot be collected by schools and districts, and/or disclosed to non-governmental private entities outside the school, district or state;

3. The extent to which the state department of education itself is prohibited from collecting certain kinds of sensitive student data, including health, disability, and disciplinary information, from schools or districts;

4. The extent to which state departments of education and/or school districts are prohibited from disclosing student data to the federal government or its designees, including researchers, without consent;

5. The extent to which private entities receiving or collecting student data are

[7] Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices. The U.S. Department of Education Established the Privacy Technical Assistance Center (PTAC), studentprivacy.ed.gov/.

permitted to develop student profiles based on their personal information;

6. The extent to which private entities receiving student data from schools or directly from students are permitted to disclose the data to additional parties such as sub-contractors; and

7. The extent to which these sub-contractors or other parties receiving or collecting student data from private entities are permitted to redisclose to yet additional organizations, companies or individuals.

The summary of state grades in parental and student data rights is listed in **Figure 7**.

Colorado and New Hampshire received the highest mark of "B+" for providing parents and students with some control over the disclosure and use of their personal data. Of those states that have student privacy laws, Idaho, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, and Wyoming received "F"s for failing to restrict the collection and use of student data.

FIGURE 7 - Parental and Student Data Rights Grade Summary

Grade	# States	State Names
A+	0	None
A	0	None
A-	0	None
B+	2	Colorado, New Hampshire
B	1	Tennessee
B-	3	California, Georgia, North Carolina
C+	2	Kansas, West Virginia
C	9	Arizona, Connecticut, Delaware, Hawaii, Illinois, Maine, Michigan, Nebraska, Virginia
C-	8	Arkansas, Florida, Indiana, Missouri, Nevada, New York, South Dakota, Utah
D+	5	District of Columbia, Maryland, Oregon, Texas, Washington
D	3	Iowa, Kentucky, Louisiana
D-	0	None
F	18	Alabama, Alaska, Idaho, Massachusetts, Minnesota, Mississippi, Montana, New Jersey, New Mexico, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Vermont, Wisconsin, Wyoming

Limitations on Commercial Use of Data

In May 2017, an article in *The Economist* declared that data has replaced oil as the most valuable resource in the world, and that the five most valuable "giants that deal in data" include Alphabet (Google's parent company), Amazon, Apple, Facebook and Microsoft.[8] Not surprisingly, each of those companies also holds a considerable share of the market for educational devices and software, although there are many other smaller ed tech companies competing for a profitable portion of it.

Student data can be monetized and commercialized by companies in various forms. Data can be sold outright; it can be transferred in mergers, acquisitions, and bankruptcies; and it can even be sold piecemeal via an asset sale. Some companies sell personal student data in the form of a "license"; meaning they disclose it for a fee under certain conditions, though the oversight to ensure that these conditions are complied with may be weak or non-existent. Companies may also mine personal student data to improve their existing products and services, and to develop new ones. They can analyze the data to identify patterns, to predict new consumer trends, and/or to market directly to children and families.

In our view, none of these practices should be allowed by schools or their vendors without the informed consent of students and/or their parents because they do not directly benefit their education. Even with consent, these practices should probably be barred. [See the box on consent on page 13].

We therefore gave high grades to states whose laws attempt to keep personal student data safe from commercial purposes, and low grades to states that prohibit none of these practices.

We used the following five measurable factors to determine each state's grade for restricting the commercialization of student data:

1. Education agencies are prohibited from selling student data;

2. Private entities, including school vendors and contractors, are prohibited from selling student data;

3. Private entities are prohibited from using student data for targeted advertising or other marketing purposes;

4. Private entities are prohibited from using student data for other commercial purposes including to

[8] "The World's Most Valuable Resource Is No Longer Oil, but Data." The Economist, The Economist Newspaper, www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

improve or develop their services or products; and

5. Private entities are prohibited from using even "de-identified" or aggregate student data for commercial purposes, including to develop new services or products, since de-identified data can often be re-identified, through access to other large data sets and other publicly released data.

The summary of state grades in limiting the commercial use of data is listed in **Figure 8**.

New York received the highest mark of "A-" for prohibiting the commercial use of student data and a limited set of teacher and principal data. Of those states that have student privacy laws, Florida, Indiana, North Dakota, Ohio, Oklahoma, Pennsylvania, South Dakota, West Virginia, and Wyoming received "F"s for not placing any restrictions on commercial uses of data. Points were deducted, and "F"s were also awarded to Michigan and Louisiana for deliberately allowing the sale of student data without parental consent in certain circumstances. For example, Louisiana allows public and private entities with access to student data to "sell, transfer, share, or process any student data for use in commercial advertising, or marketing" if such activity is permitted in the vendor's contract.

On the issue of "de-identification of data"

The re-identification of individuals is possible when data is not sufficiently de-identified or aggregated, particularly with large data sets. For example, in 1997, Massachusetts Governor William Weld ordered the health records of state employees to medical researchers, after their names, addresses, and Social Security numbers were removed. His administration assured the public that stripping (or de-identifying) the information would make it impossible for anyone to identify individual patients. Yet Latanya Sweeney, then a graduate student of the Massachusetts Institute of Technology and now a Harvard professor, was able to positively identify the health records of the governor himself within only a few days, by using remaining data including date of birth, sex and zip code, and cross-referencing it with other public data such as voter registration records.

FIGURE 8 - Limitations on Commercial Use of Data Grade Summary

Grade	# States	State Names
A+	0	None
A	0	None
A-	1	New York
B+	0	None
B	1	Colorado
B-	4	Kentucky, New Hampshire, Tennessee, Virginia
C+	0	None
C	19	Arizona, Arkansas, California, Connecticut, Delaware, Georgia, Hawaii, Illinois, Iowa, Kansas, Maine, Missouri, Nebraska, Nevada, North Carolina, Oregon, Rhode Island, Texas, Washington
C-	0	None
D+	3	District of Columbia, Idaho, Maryland
D	1	Utah
D-	0	None
F	22	Alabama, Alaska, Florida, Indiana, Louisiana, Massachusetts, Michigan, Minnesota, Mississippi, Montana, New Jersey, New Mexico, North Dakota, Ohio, Oklahoma, Pennsylvania, South Carolina, South Dakota, Vermont, West Virginia, Wisconsin, Wyoming

Data Security Requirements

Unlike the banking and financial industries that by law must comply with strict data security standards, the safety and security of education data is largely unregulated by the federal government. Student data was traditionally considered a low-value target for data hackers and identity thieves because their records rarely contain detailed financial information, such as bank account or credit card numbers.

It turns out, however, that student data includes valuable information for identity theft, including social security numbers and mother's maiden names. Because very few children have negative credit histories, identity thieves intent on acquiring it may be willing to wait one or two years to open credit files and cash in. According to a recent Carnegie Mellon report, identity protection scans of over 40,000 children 18 and under revealed that 10.2 percent had their Social Security numbers stolen – 51 times higher than the rate of adults in the same study.[9]

Moreover, there has also been a sharp increase in recent years of ransomware attacks on schools and higher education institutions, in which a hacker takes control of the student information systems, preventing schools from accessing these systems until

[9] Power, Richard. "Child Identity Theft." Carnegie Mellon CyLab, www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf.

they pay a considerable sum of money. For the first time, the education sector has outpaced the government, retail, and healthcare industries in ransomware attacks.

There have been 389 cyber security-related incidents in U.S. K-12 public schools alone between January 2016 and November 2018.[10] Although protecting data may be costly, data breaches are far more expensive. In 2017, the average cost of a data breach in education was $245 per compromised record.[11] And this does not account for the priceless loss of a child's personal privacy.

We gave high grades to states that require education agencies and the private entities that have access to student data to implement rigorous data cybersecurity measures and to notify parents promptly of any breaches.

Grades were assigned using the following three factors:

1. The extent to which education agencies are required to implement a data security program, including, but not limited to, encryption, security audits, audit logs, data retention and destruction procedures, and training;

2. The extent to which private entities collecting or receiving student data are required to implement such practices; and

3. The extent to which education agencies and/or private entities including third-party contractors must notify parents of data breaches.

The summary of state grades for strong data security protections is listed in **Figure 9**.

New York received the highest mark of "B+" for requiring educational agencies and private entities to take precautions to secure student, teacher and principal data. Of those states that have student privacy laws, Florida, Kentucky, Ohio, Pennsylvania, and Rhode Island were awarded "F"s for failing to include any requirements in law to protect data from unauthorized disclosures.

[10] K-12 Cyber Incident Map – EdTech Strategies. EdTech Strategies, www.edtechstrategies.com/k-12-cyber-incident-map/.

[11] Schaffhauser, Dian. "Average Cost Per Record of US Data Breach in Ed: $245." Campus Technology, 18 July 2017, campustechnology.com/articles/2017/07/18/average-cost-per-record-of-us-data-breach-in-ed-245.aspx.

FIGURE 9 - Data Security Requirements Grade Summary

Grade	# States	State Names
A+	0	None
A	0	None
A-	0	None
B+	1	New York
B	0	None
B-	3	Colorado, North Carolina, Tennessee
C+	5	Georgia, Idaho, Nevada, Utah, West Virginia
C	5	Connecticut, District of Columbia, Missouri, Oklahoma, Virginia
C-	6	Delaware, Indiana, Kansas, Louisiana, North Dakota, Wyoming
D+	0	None
D	13	Arizona, Arkansas, California, Hawaii, Illinois, Iowa, Maine, Maryland, Michigan, Nebraska, Oregon, Texas, Washington
D-	2	New Hampshire, South Dakota
F	16	Alabama, Alaska, Florida, Kentucky, Massachusetts, Minnesota, Mississippi, Montana, New Jersey, New Mexico, Ohio, Pennsylvania, Rhode Island, South Carolina, Vermont, Wisconsin

Oversight, Enforcement, and Penalties for Violations

FERPA applies to all states, districts and schools that receive funds from the U.S. Department of Education.[12] When a parent alleges that a district or school has violated FERPA and submits a complaint to the Department, this may trigger an investigation. If then a determination is made that the district or school violated FERPA, school officials are informed of the steps they must take to come into compliance with the law.[13] If the school does not comply, the Department may withhold federal funds. However, the federal government is years behind in responding to FERPA complaints and has never withheld funds from any school or district for violations. Moreover, as described above, FERPA was designed for a pre-digital age and has been weakened through regulatory action over the years. Thus, rigorous enforcement action to protect student privacy is critical at the state level.

We gave high grades to states with laws that clearly identify who is responsible for oversight, describe a specific process for enforcement, and enumerate penalties for non-compliance.

[12] Family Educational Rights and Privacy Act (FERPA). US Department of Education (ED), 1 Mar. 2018, www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[13] FERPA for Parents. US Department of Education (ED), 26 June 2015, www2.ed.gov/policy/gen/guid/fpco/ferpa/parents.html.

The following six factors were used to determine each state's grade in this category:

1. Whether a regulating authority, other than the state department of education, is identified;
2. Whether an enforcement process is defined;
3. Whether fines/penalties for violations or breaches are enumerated;
4. Whether a state Chief Privacy Officer (CPO) or similar position is mandated;
5. Whether a citizen or stakeholder student data privacy oversight board or committee is created;
6. Whether parents or students have a right of private action to sue if their privacy is violated.

The summary of state grades for oversight, enforcement and penalties for violations is listed in **Figure 10**.

Illinois received the highest mark of "B+" for including specific enforcement and oversight mechanisms in law. Of those states that have student privacy laws, Colorado, the District of Columbia, Hawaii, Iowa, Kentucky, Maine, Maryland, Michigan, Nebraska, New Hampshire, North Dakota, Ohio, Oklahoma, Pennsylvania, South Dakota, Texas, and Washington received "F"s for failing to identify any process to enforce or entity to oversee the law other than the state department of education.

FIGURE 10 - Oversight, Enforcement and Penalties for Violations Grade Summary

Grade	# States	State Names
A+	0	None
A	0	None
A-	0	None
B+	1	Illinois
B	0	None
B-	1	Idaho
C+	0	None
C	5	Arizona, Delaware, Missouri, Nevada, Utah
C-	8	Connecticut, Florida, Indiana, Kansas, Louisiana, North Carolina, Rhode Island, Tennessee
D+	0	None
D	8	Arkansas, California, Georgia, New York, Oregon, Virginia, West Virginia, Wyoming
D-	0	None
F	28	Alabama, Alaska, Colorado, District of Columbia, Hawaii, Iowa, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, North Dakota, Ohio, Oklahoma, Pennsylvania, South Carolina, South Dakota, Texas, Vermont, Washington, Wisconsin

Other Provisions

State student privacy laws are complex and some features of these laws, while important, did not fit into any of our categories. Some provisions revise or repeal existing code, some introduce a new section to existing law, and others stand alone as entirely new statutes.

We gave additional points to states that had laws with provisions that did not fit in any of the above categories but would help protect student privacy, while subtracting points from those states with laws that would adversely affect privacy in other ways. Some examples include:

- New Hampshire was awarded additional points for requiring consent prior to including state exam scores in student transcripts:

  > "*The statewide assessment results of a student or the student's school district shall not be included as part of the student's transcript unless the student, if 18 years of age or older, or the student's parent or legal guardian if the student is under 18 years of age, consents.*"

- Delaware received extra credit for prohibiting schools and employees from receiving compensation for recommending the use of ed tech products:

> "*The Department, school district, or school may recommend, solely for the K-12 school purposes, any educational materials, online content, services, or other products to any student or to the student's family if the Department, school district, or school determines that such products will benefit the student and no person receives compensation for developing, enabling, or communicating such recommendations.*"

- Louisiana received additional points for barring contractors from using "predictive modeling" to direct a child's educational career:

> "*No contractor shall use student information to conduct predictive modeling for the purpose of directing the educational opportunities of students.*"

- On the other hand, North Dakota lost points because its law allows the state to actively solicit non-governmental funding for its student longitudinal database, which places student data at additional risk because private interests may then have undue influence over which information is collected and how it can be used:

> "*The statewide longitudinal data system committee may solicit and receive gifts, grants, and donations from public and private sources. Any moneys received in accordance with this section are appropriated on a continuing basis for the support of the statewide longitudinal data system.*"

The summary of state grades for other provisions that do not fit into our general categories is listed in **Figure 11**.

For more details on unusual features of state privacy laws leading to the addition or subtraction of points, check our comparison matrix.

New Hampshire received the highest mark of "B+" in the other provisions category for including additional protections for privacy. Of those states that have student privacy laws, Georgia, Kentucky, Ohio, and South Dakota received "F"s for scoring zero points in this category. Points were deducted, and "F"s were also awarded to Arizona, Arkansas, California, Connecticut, the District of Columbia, Hawaii, Indiana, Iowa, Kansas, Maryland, Michigan, Nebraska, Nevada, North Carolina, North Dakota, Oregon, Texas, and Washington for including provisions that placed privacy at risk.

For more details, please refer to the comparison matrix of state laws and the Technical Appendix.

FIGURE 11 - Other Provisions Grade Summary

Grade	# States	State Names
A+	0	None
A	0	None
A-	0	None
B+	1	New Hampshire
B	0	None
B-	0	None
C+	2	Louisiana, Tennessee
C	1	Colorado
C-	0	None
D+	4	Idaho, Illinois, Rhode Island, West Virginia
D	4	Missouri, New York, Oklahoma, Wyoming
D-	6	Delaware, Florida, Maine, Pennsylvania, Utah, Virginia
F	33	Alabama, Alaska, Arizona, Arkansas, California, Connecticut, District of Columbia, Georgia, Hawaii, Indiana, Iowa, Kansas, Kentucky, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, Oregon, South Carolina, South Dakota, Texas, Vermont, Washington, Wisconsin

On the issue of Teacher Data Privacy Protections

While student privacy has received a great deal of attention since 2013, teacher data privacy has been largely ignored. When a state had a law that specifically protected teacher and/or administrator privacy, it was awarded additional points under the "Parties Covered and Regulated" category and assigned points in other categories accordingly. For details, see the "Teacher Provisions" section of the comparison matrix.

Of the 99 privacy laws we evaluated, only three states enacted laws that attempted to meaningfully protect teacher personal data: New Hampshire, New York, and Tennessee. For example, New Hampshire requires school board approval and the written consent of both ***teachers*** and parents before a classroom can be video- or audio-recorded for use in teacher evaluations. In Tennessee, the state board of education must develop a detailed security plan including access controls to the ***teacher*** data system and develop guidelines for accessing individual ***teacher*** data. New York prohibits personally identifiable information (PII) maintained by educational agencies, including data provided to third-party contractors and their assignees, from being sold or used for marketing purposes. PII, as applied to ***teachers*** or principals in this case, means information in an educator's records relating to his or her annual performance reviews.

PARENT COALITION FOR STUDENT PRIVACY

www.studentprivacymatters.org

THE NETWORK FOR PUBLIC EDUCATION

www.networkforpubliceducation.org