Parent Toolkit
for Student Privacy

A Practical Guide for Protecting
YOUR CHILD'S SENSITIVE SCHOOL DATA
from Snoops, Hackers, and Marketers

PARENT COALITION FOR STUDENT PRIVACY

ccfc
Campaign for a Commercial-Free Childhood

MAY 2017

TABLE OF CONTENTS

INTRODUCTION
Why should parents be concerned?

It's difficult for parents to imagine just how much information is collected about students in schools today, or how that information is used, stored, and shared with others. During the course of a normal school day — and throughout a child's life from kindergarten to graduation from high school — an incredibly large amount of data, including highly sensitive information, is shared without parental knowledge or consent with vendors providing operational services or companies offering educational programs. Rather than secured in a file cabinet or kept on the school's computer servers, personal student information is often transmitted to and stored in the "cloud" to facilitate access and use by third parties. Federal laws intended to protect students' data held by or for schools are simply inadequate to address the challenges of today's digital age.

Parents may never know the full extent of how their children's personal information may have been shared, used, misused, sold, breached, or hacked over the course of their school careers. If their children are denied entrance into the college of their choice, parents may wonder if their students' profiles were sold to universities by the College Board and ACT and used to reject their application. If their children are turned down for their dream jobs, did the employer screen them using an online profile of their internet search history gathered by their school-issued device and bought from data brokers? If their children's identities are stolen, was it the result of an elementary school's data breach many years ago? If their children are denied state services as an adult, could it be because of disciplinary or other incriminating information in their cumulative files held by the state education department and other agencies?

This toolkit is designed to help parents like you navigate these issues, and provide information on your rights and what steps you can take to maximize your children's privacy and safety. As parents understand instinctively, it is your job to protect your children and try to ensure their success in school and life. We hope this toolkit will help you.

Acknowledgments

This effort was a joint project of the Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood, and was made possible by a generous grant from the Rose Foundation for Communities and the Environment's Consumer Privacy Rights Fund.

The Parent Toolkit for Student Privacy was authored by Rachael Stickland, Melissa Campbell, Josh Golin, Leonie Haimson, and David Monahan, and designed by Ross Turner Design. Special thanks to advisory members Kris Alman, Oregon Education Advocate; Faith Boninger, National Education Policy Center, University of Colorado Boulder; Laura Bowman, Parents Across America; Phyllis Bush, Co-founder of Northeast Indiana Friends of Public Education, and Board member, Network for Public Education; Tim Farley, New York State Alliance for Public Education; Jennifer Jacobson, Connecticut Alliance for Privacy in Education; Cheri Kiesecker, Parent Coalition for Student Privacy; Chad Marlow, American Civil Liberties Union*; Francesca Miceli, Esq.; Mark B. Miller, School Director, Centennial, Pennsylvania School District, and Board member, Network for Public Education; and Sarah Petrie, Esq.*

** Affiliation for identification purposes only*

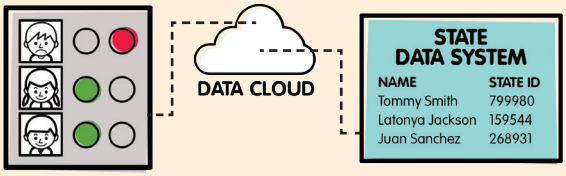
Questions? Visit www.studentprivacymatters.org/toolkit for more information, including free webinars on how to use the resources in this toolkit.

SECTION I.

What is student data?

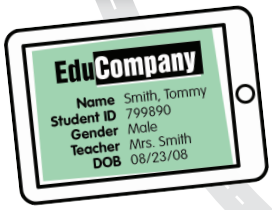
To fully understand the types and amount of personal information a student generates in today's digital world, and how it's used and shared, let's examine the life of a fictitious child named Tommy and his journey through a data- and technology-driven school experience.

1. Before he starts kindergarten, Tommy's parents must provide his school with his personal information including name; gender; date of birth; social security number; health information (e.g., immunizations, prescribed medications, disabilities, allergies, etc.); and family income information to see if he qualifies for free or reduced-priced lunch.



Tommy's information is then uploaded into the district's online database — which is likely maintained by an out-of-state company such as InfiniteCampus and stores all data in the "cloud" — and provided to school administrators, teachers, and parents via a digital "data dashboard."

The school will send much of the information electronically to the state department of education to track Tommy's progress through school in the statewide longitudinal data system (SLDS). Researchers and policymakers often use this information for accountability and evaluation purposes.



2. Before Tommy arrives in the classroom for his first day, his personal information is shared with various companies that provide services to the school and district. The district creates Tommy's school bus and online lunch account and ID card, and signs him up with Google's G Suite for Education.

3. On his way to school, Tommy's location and internet activity are tracked by technology installed on his school bus.

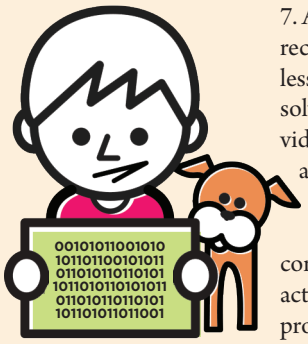
A radio frequency identification (RFID) chip in Tommy's ID card allows the school to track his whereabouts.

If Tommy allows his smartphone or tablet to connect to the Wi-Fi while riding on the bus, his login and browsing information may be tracked by the internet provider and school district.

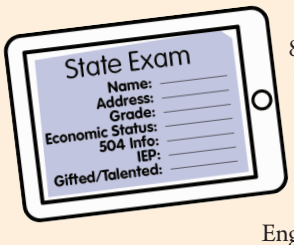
4. While in class, if Tommy speaks without raising his hand, his teacher records the event in his Class Dojo account — an online behavior management tool. The system emits an audible "BONG" for the entire class to hear and adds a demerit to his online profile. Daily and weekly updates are sent to Tommy's parents via a phone app, text, or email.

5. In the cafeteria, Tommy provides his fingerprint, name, or student number to the lunchroom aide, who then records his food selections in his online account, which may become a part of his permanent digital record.

6. During gym class, Tommy wears a heart rate monitor to record his workout intensity as part of his grade. An app analyzes the results and sends a report via email to the teacher's Dropbox account. It's unclear what happens to Tommy's digital health information at the end of the school year.



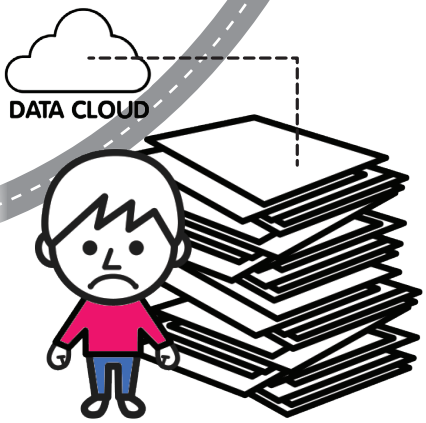
7. At home and school, Tommy receives "personalized learning" lessons online. Whether he's solving math problems via a video game or taking quizzes after reading a story, for-profit technology companies — *not* his teachers — determine the content and difficulty level of the activity by collecting data and using proprietary algorithms to analyze his abilities, profile his interests, and predict outcomes. This process is known as "data mining."

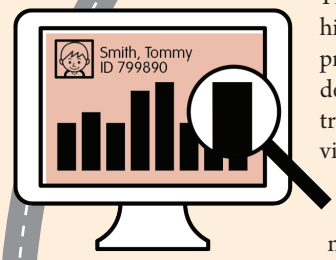


8. Starting as early as Kindergarten, Tommy is assigned interim assessments or test prep to meet district and state requirements. In grades 3 through 8, he takes annual standardized exams in math and English Language Arts (ELA) as required by federal law. He may also be subjected to various local and periodic standardized assessments in these and other subjects. Companies administering these tests often collect an array of sensitive personal information from students, as well as metadata like the amount of time they spend answering a specific question. Essays are often scored by machines rather than people.

9. Sometime during elementary school, Tommy may be asked to complete "school climate" and other surveys measuring his personal beliefs, his political views, or social and emotional skills, often using an online account with his name or other personal information attached to it.

10. As Tommy progresses through his elementary and middle school years, his education record grows to include grades, course schedules, standardized test scores, disciplinary information, counseling records, disabilities and 504 or Individualized Education Plans, and any health condition he might have that requires medication or special treatment in school. The file may also include information on his family history, his racial and ethnic background, his country of birth, whether he is an immigrant or homeless, and what special services he receives.





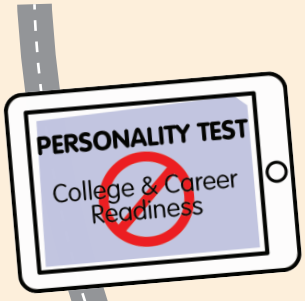
11. When Tommy reaches sixth grade or even sooner, his district may implement a 1:1 program. District-provided devices will be issued to each student with default settings that allow companies like Google to track and mine student data, including internet sites visited and search terms used, books and articles read online, videos watched on YouTube, and passwords. Tommy uses this device until he graduates, amassing millions of data points that can be mined to diagnose his learning issues, steer him towards certain courses or careers, or generate a consumer profile that can be sold by data brokers.

12. Without the knowledge or consent of his parents, Tommy's school district may share his name, course grades, attendance records, disciplinary records, standardized test scores, and disabilities with private researchers and even the U.S. Department of Education. Study results will never be provided to Tommy or his family.

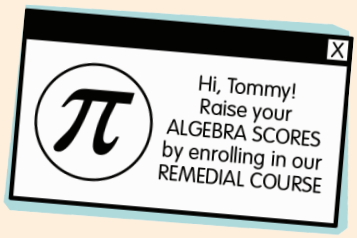
WHAT ARE THE FACTS ABOUT "PERSONALIZED LEARNING" PRODUCTS?
According to a 2016 paper by the Data & Society Research Institute, "Most product websites describe the input of teachers or learning scientists into development as minimal and after the fact (Guernsey & Levine, 2015). Products are not field tested before adoption in schools and offer limited to no research on the efficacy of personalized learning systems beyond testimonials and anecdote."[1]

HOW DO PARENTS FEEL ABOUT STUDENT PRIVACY? A 2015 study by the Future of Privacy Forum found that 87% of parents surveyed "worry about student data being hacked or stolen." The study also found that 68% of parents surveyed are concerned "that an electronic record would be used in the future against their child by a college or an employer."[2]

WHAT HAPPENS TO DATA CAPTURED ONLINE?
When students browse the internet – whether at home or school – their information is collected by online companies, bundled as consumer profiles, and then sold in the shadowy data market. Because this data has the potential to accurately predict feelings, motivations, and behaviors, it may be purchased by colleges, employers, mortgage lenders and insurance underwriters to evaluate an individual's suitability for those services and products.

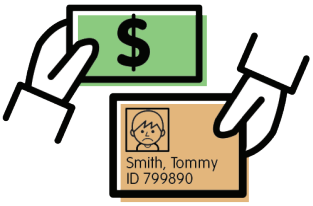


13. By the time Tommy is in middle school, he is encouraged or required to use an online program like Naviance to complete surveys and set personal and academic goals to plan for college. Once in high school, he will be required to use much of the information stored in Naviance to apply for college.

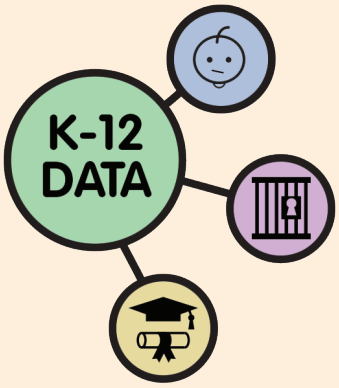


14. In high school, Tommy registers for an online course or instructional app in addition to his traditional classes. Some online courses, like those offered by a company called Knewton, collect millions of data points on each student per day. Information Tommy provides online companies may be used to advertise products or programs to him or his parents, based on his personal data.

15. In high school, Tommy takes College Board Advanced Placement (AP) courses and exams, the PSAT, SAT, and/or the ACT, before which he will be asked a series of personal questions. The College Board or ACT may then sell his student profile to colleges to help them decide whether to recruit and admit him or not, if he unknowingly gives his consent.

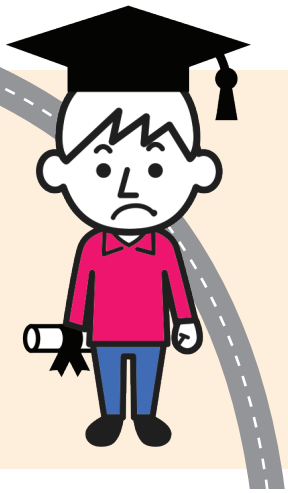


16. When Tommy is a sophomore or junior, his private information may be shared with military recruiters unless his parents revoke their permission in writing. Regardless, his school may administer the Armed Services Vocational Aptitude Battery (ASVAB) exam and release his results to recruiters.



18. By the time Tommy graduates, his education record spans more than 13 years. Each year of school, his district sent much of the information in his record to the statewide longitudinal data system (SLDS) where it may be linked to other state agency databases, including the departments of health and human services, higher education, and corrections, and then passed along to researchers.

At any point in Tommy's educational career, his personal data, whether held by his school, state or federal agencies, researchers, or online vendors, may have been misused, breached, or hacked, damaging his future prospects in ways beyond our current imagination.



HAS STUDENT DATA STORED IN STATE SYSTEMS OR SLDS BEEN MISUSED? In March 2016, a judge ordered the records of 10 million California students, including "names, addresses, disciplinary records, grades, test scores, and even details such as pregnancy, addiction and criminal history," to be made available to a private organization suing the state for access to the student database.[3]

HAS STUDENT DATA BEEN BREACHED BY SCHOOLS? In February 2016, Washington D.C. Public Schools publicly posted the private information of approximately 12,000 public school special needs students online, including "each student's identification number, race, age, school, disabilities and any services he or she receives."[4]

DO COMPANIES OFFERING ONLINE "LEARNING" PRODUCTS GET HACKED? In late 2015, VTech, an "award winning electronic learning toy company," had 4.9 million parent accounts and 6.4 children profiles breached by a hacker. Parent information included "name, mailing address, email address, IP address, download history and account credentials." Child profiles included name, gender, and birthdate.[5]

Questions? Visit www.studentprivacymatters.org/toolkit for more information, including free webinars on how to use the resources in this toolkit.

REFERENCES

1. https://datasociety.net/pubs/ecl/PersonalizedLearning_primer_2016.pdf

2. https://fpf.org/wp-content/uploads/2015/11/Beyond-the-Fear-Factor_Sept2015.pdf

3. http://www.mercurynews.com/bay-area-news/ci_29590794/judge-pulls-back-from-calif-student-records-release

4. https://www.washingtonpost.com/local/education/dc-accidentally-uploads-private-information-of-12000-students/2016/02/11/7618c698-d0ff-11e5-abc9-ea152f0b9561_story.html

5. https://www.washingtonpost.com/news/the-switch/wp/2015/12/01/vtech-says-6-4-million-children-were-caught-up-in-its-data-breach/

SECTION II.

Parents' rights under federal law to protect their children's privacy

Knowing your rights under the complicated patchwork of federal laws, state statutes, and local policies governing the use and disclosure of a student's personal information can be challenging. In this section, we briefly describe the federal laws known as **FERPA** (Family Educational Rights and Privacy Act), **NSLA** (National School Lunch Act), **IDEA** (Individuals with Disabilities Education Act), **PPRA** (Protection of Pupil Rights Amendment), and **COPPA** (Children's Online Privacy Protection Act).

Federal laws currently provide a baseline for protecting student privacy. In recent years, members of Congress have introduced many bills attempting to strengthen student privacy protections, but as of April 2017, none have passed.

Many states have passed laws in recent years that enhance student privacy. Become familiar with the student privacy laws in your state and monitor them closely for changes. For updates on federal bills, and new state student privacy laws, visit www.parentcoalitionforstudentprivacy.org and subscribe to our newsletter.

Local school districts and state departments of education can and should do their part to develop student privacy policies and procedures that reach beyond protections offered in federal or state law. We offer suggestions in Section IV.

FERPA (Family Education Rights and Privacy Act)

Passed in 1974, the **Family Educational Rights and Privacy Act (FERPA)** (20 U.S.C. § 1232g; 34 CFR Part 99) is administered by the U.S. Department of Education and applies to federally-funded schools and universities. It bars the disclosure of personally identifiable information (PII) in student education records—like grades, test scores, disciplinary records, contact and family information, and class schedules—to third parties without parental consent, but with some loopholes described below. The law has been considerably weakened through regulatory changes in the past ten years, and was written before the emergence of computerized data systems and data-collecting learning software. Both of these factors allow student PII to be easily shared with others outside of the school.

Per the U.S. Department of Education, "disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record."

The U.S Department of Education's definition of "Personally Identifiable Information (PII)" includes, but is not limited to: a student's name; the name of the student's parent or relatives; physical address; personal identifier such as a social security number or student ID number, or biometric record; other indirect identifiers such as date of birth, place of birth, mother's maiden name; or other information that, alone or in combination, is linked or linkable to a student, allowing others to identify the student.

FERPA contains multiple "exceptions," or certain circumstances under which student PII may be disclosed to parties outside of the school or district without parental consent. The most widely used is the "school official" exception, which allows student PII to be shared with vendors, consultants, contractors, and volunteers with "legitimate educational interests" who are performing "institutional services or functions" for the school. Common examples include online instruction and assessment providers, bus or cafeteria service companies, vendors that provide student information systems, and parents or other classroom volunteers. The "audit and evaluation" exception also allows disclosure without parental consent to "authorized representatives" of "Federal, State, and local educational authorities conducting an audit, evaluation, or enforcement of education programs." This exemption allows for the development of statewide longitudinal data systems (SLDS) where student data may be shared among various state agencies, including health and human services, corrections,

public safety, and labor and workforce.[1] A third broad exception allows nonconsensual disclosures of student PII to organizations or individuals for research purposes or "studies." These studies must be limited to the purpose of "developing, validating, or administering predictive tests; administering student aid programs; or improving instruction." For more on FERPA, visit http://bit.ly/SPTK_FERPA [2]

Per the U.S. Department of Education, "education records" are records that directly relate to a student and are maintained by the school or a party acting for the school.

Education records "include but are not limited to grades, transcripts, class lists, student course schedules, health records (at the K-12 level), student financial information (at the postsecondary level), and student discipline files. The information may be recorded in any way, including, but not limited to, handwriting, print, computer media, videotape, audiotape, film, microfilm, microfiche, and e-mail."

Education records also include a record of any student personal information requested by or disclosed to:
1. Organizations conducting "studies" for or on behalf of the school;
2. Federal, State or local educational authorities; and
3. Unauthorized third parties including any instances of security breaches or hacks.[3]

What rights do parents have under FERPA?

1. PARENTS HAVE THE RIGHT to access the information in their child's education records held by the state education department, the local district, and/or the school. The state, district, and school cannot charge parents a fee to search for or to retrieve education records, but they may apply a reasonable fee to provide copies of education records, and must provide them in a readable format within 45 days of receiving a request from parents. Note that some states have laws that require production of records within a shorter period of time. Parents may need to complete a specific form found on the state, district, or school website to access education records, or they may need to call the state, district, or school office for more information. If a form is not provided, see Appendix A for a sample.

2. PARENTS CAN REQUEST to correct information in their child's records if they believe it is "inaccurate, misleading, or in violation of the privacy rights of the student." If the school, district, or state refuses to correct the record, parents have the right to a formal hearing. If after the hearing, the school, district, or state still refuses to correct the record, parents have the right to amend the record by placing in it a statement setting forth their view of the contested information.

3. PARENTS HAVE THE RIGHT to be informed of the school and/or district's criteria for determining who constitutes a "school official," or other third party with a "legitimate educational interest," to whom the school and/or district may disclose PII without parental notification or consent.

Schools often designate companies that host online programs or classroom apps as "school officials."

4. PARENTS HAVE THE RIGHT to opt out of "directory information" about their child being offered to third parties by the school or district. Directory information generally includes a more limited set of personal information that is not considered highly sensitive. Note that opting out of "directory information" does not prevent schools or districts from disclosing personal student data, often of an even more sensitive nature, to "school officials," "authorized representatives," or "organizations" under the exceptions noted above. For information on how to opt out of directory information, see Appendix B.

"Directory information" includes but is not limited to the student's name, address, telephone, email address, photo, date and place of birth, major field of study, grade level, enrollment status, date of graduation, participation in activities and sports, weight and height, degrees, honors and awards received, and the most recent school attended.

Directory information does not include a student's social security number, or a student identification (ID) number if that number alone is enough to identify the student.

5. PARENTS HAVE THE RIGHT to opt out of having their child's "contact information" provided to military recruiters. To do so, parents must submit a written request to the school. For a sample form, see Appendix C.

6. SCHOOLS OR DISTRICTS MUST INFORM PARENTS annually of their FERPA rights. The actual means of notification (e.g., email, letter, PTA bulletin, student handbook, or website) is left to the discretion of each school.

7. A STUDENT'S PERSONAL INFORMATION CANNOT BE INDISCRIMATELY SHARED even within the school setting. Instead, disclosure should be limited to those teachers and other school employees directly responsible for the student's education

or services, who "need to know" students' information in order to be able to fulfill their professional responsibilities.

Per the U.S. Department of Education, "[a]n 'eligible student' means a student who has reached the age of 18 or who is attending a postsecondary institution at any age."

NOTE: The rights of parents under FERPA transfer to a student who reaches 18 years old or attends a postsecondary institution (e.g., college or university), or becomes an emancipated minor under state law.

If you believe that you or your child's rights under FERPA have been violated, notify your school, district Superintendent, and/or school board. If they refuse to take appropriate action, you may contact your local chapter of the American Civil Liberties Union (ACLU) to request help, or file a complaint with the U.S. Department of Education's Family Policy Compliance Office. A FERPA complaint must be in writing and contain specific instances giving reasonable cause to believe that a privacy violation has occurred; filed by the parent of a student at an elementary or secondary school under the age of 18 or an eligible student; and filed within 180 days of the alleged violation or within 180 days after the complainant knew or should have known about the violation. For more information or to file a complaint, visit http://familypolicy.ed.gov/complaint-form

IDEA (Individuals with Disabilities Education Act)

To learn more about some of the additional privacy rights of children with disabilities, see http://bit.ly/SPTK_IDEA_FERPA [4]

The **Individuals with Disabilities Education Act (IDEA)** (Public Law No. 94-142) is designed to protect the rights of children with disabilities, including students with Individualized Education Programs or IEPs, to be provided with a free and appropriate education. The law is administered by the U.S. Department of Education. Children with disabilities have additional privacy rights under IDEA. For example:

1. PARENTAL CONSENT IS REQUIRED before the PII of a child with disabilities can be released to participating agency officials providing or paying for secondary transition services which are designed to facilitate a student's movement from school to post-school activities.

2. PARENTAL CONSENT MUST BE OBTAINED if a public school child enrolls in a private school in a different district from the parents' residence before the child's PII can be disclosed to the district in which the private school is located.

3. PARENTS MUST GIVE PRIOR WRITTEN CONSENT each year before the district can disclose a child's special education service records to the State Medicaid agency for the purposes of claiming reimbursement from the federal government. Parents can withdraw their consent for this disclosure at any time, and the district must provide the child with mandated services whether or not consent is given.

NOTE: For more information, contact your school district, local special education director, or state special education director or visit the IDEA website at http://bit.ly/SPTK_IDEA [5]

If you believe that you or your child's privacy rights under IDEA have been violated, notify your school, district Superintendent, and/or school board. If they refuse to take appropriate action, you should contact your state education department. You may also contact your local chapter of the American Civil Liberties Union (ACLU) to request help, or file a complaint

with the U.S. Department of Education's Family Policy Compliance Office. For more information or to file a complaint, visit http://familypolicy.ed.gov/complaint-form

NSLA (National School Lunch Act)

The **National School Lunch Act (NSLA)** of 1946 (79 P.L. 396, 60 Stat. 230) is administered by the U.S. Department of Agriculture (USDA). It applies to all schools receiving federal education funds, and protects confidential eligibility and income information collected by schools to determine whether a child may receive free or reduced-priced lunch (FRL) or free milk under the National School Lunch Program. For more on NSLA, visit http://bit.ly/SPTK_NSLA [6]

What rights do parents have under NSLA?

1. PARENTS MUST PROVIDE prior consent before the disclosure of FRL eligibility information to: 1) local education and health programs; and 2) State and Federal health programs other than Medicaid or the State Children's Health Insurance Program (SCHIP). Parents must also be given prior notice and the opportunity to decline to have eligibility information disclosed to Medicaid or SCHIP.

"Eligibility information" generally includes but is not limited to personal information about household size and family income; versus "eligibility status" which designates whether a child is eligible or not eligible for FRL.

2. A STUDENT'S ELIGIBILITY information cannot be made available to all school employees; rather, disclosure should be limited to the teachers, tutors, or other school officials directly responsible for a child's education and care. Additionally, a school's student information system (SIS) and/or computer screens or rosters used in the cafeteria must mask or otherwise de-identify a student's eligibility status to prevent others from accessing or viewing it — especially other students.

For example, if a local non-profit organization or recreation program would like to offer free textbooks or summer athletic classes based on a child's FRL status, parents must first consent to allow their school to disclose their children's eligibility information.

3. "OVERT IDENTIFICATION" of FRL students is prohibited by NSLA, including:
   - Publicizing or announcing eligible families' or children's names;
   - Having separate dining areas, service times, or serving lines; or
   - The use of meal cards, tickets, tokens, or other methods to obtain reimbursable meals (e.g., coded or colored) in a manner that would overtly identify FRL eligible children.

A Kansas school district reportedly allowed unauthorized employees to illegally view the eligibility status of students via the district's student information system. Teachers later publicly posted this information on "data walls" in apparent violation of NSLA and FERPA.[7]

4. SCHOOLS MAY DISCLOSE aggregate information that does not identify individuals (e.g., a report on the number of children eligible for FRL in a school district) without written consent of the students' parents.

NOTE: Confidential eligibility information collected from children and families applying to other USDA Child Nutrition Programs is also protected from unauthorized disclosure, including the School Breakfast Program (SBP),[8] Special Milk Program (SMP),[9] the Summer Food Service Program,[10] and the Child and Adult Care Food Program.[11]

If you believe that your child's rights under NSLA have been violated, notify your school, district Superintendent and/or school board. If they refuse to take appropriate action, you may contact your local chapter of the American Civil Liberties Union (ACLU) to request help, or file a complaint with the USDA. For more information and to access the form, visit http://www.ascr.usda.gov/complaint_filing_cust.html.

PPRA (Protection of Pupil Rights Amendment)

The **Protection of Pupil Rights Amendment (PPRA)** (20 U.S.C. § 1232h; 34 CFR Part 98) is administered by the U.S. Department of Education and was enacted in 1978. PPRA applies to the administration of student surveys, analyses, or evaluations that deal with highly sensitive issues. It also concerns marketing surveys, parental access to instructional materials, and certain physical examinations of students by schools. For more information about PPRA, visit http://familypolicy.ed.gov/ppra

PPRA allows parents to inspect: "All instructional materials, including teacher's manuals, films, tapes, or other supplementary material which will be used in connection with any survey, analysis, or evaluation as part of any applicable program."

Instructional materials include, "instructional content that is provided to a student, regardless of its format, including printed or representational materials, audio-visual materials, and materials in electronic or digital formats (such as materials accessible through the Internet). The term does not include academic tests or academic assessments."

What rights do parents have under the PPRA?

1. PARENTAL CONSENT IS REQUIRED before children are required to participate in any survey, analysis or evaluation funded by the U.S. Department of Education that concerns the following sensitive areas:
   - Political affiliations or beliefs of the student or the student's parent;
   - Mental and psychological problems of the student or the student's family;
   - Religious affiliations and beliefs;
   - Sex behavior and attitudes;
   - Illegal, anti-social, self-incriminating, and demeaning behavior;
   - Critical appraisals of close family members;
   - Legally recognized privileged relationships, such as those of lawyers, physicians, and ministers; or
   - Income (other than that required by law to determine eligibility for a program).

2. IF A SURVEY, analysis, or evaluation administered to students that deals with issues listed above is not federally-funded, written consent is not required — but parents must be notified in advance and have the right to opt their children out of participating.

3. UPON REQUEST, parents may inspect "any instructional material used as part of the educational curriculum for the student." Some schools use "character enrichment" curricula which may violate student and family privacy. Under PPRA, parents are given the specific right to review these materials.

4. PPRA REQUIRES schools to directly notify parents, at least annually at the beginning of the school year, when the following activities may occur, and grants parents the right to opt their children out of:
   - The administration of any survey containing one or more sensitive items listed above;
   - Any non-emergency, invasive physical exam or screening administered by the school unnecessary to protect the immediate health and safety of a student, except for hearing, vision, or scoliosis screenings; and
   - Activities involving collection, disclosure, or use of personal information obtained from students for marketing or to sell or otherwise distribute the information to others.

NOTE: The rights of parents under PPRA transfer to a student who reaches 18 years old or becomes an emancipated minor under State law.

Your state may allow or require your school to perform a physical examination or screening without parent notification or consent. To become familiar with your state's applicable law, be sure to ask your principal or counselor.

If you believe that you or your child's rights under PPRA have been violated, notify your school, district Superintendent and/or school board. If they refuse to take appropriate action, you may contact your local chapter of the American Civil Liberties Union (ACLU) to request help, or file a complaint similar to FERPA with the U.S. Department of Education's Family Policy Compliance Office at:

Email: FERPA.customer@ed.gov
Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-8520
Phone: 1-800-USA-LEARN (1-800-872-5327)
Fax: 202-260-9001

COPPA (Children's Online Privacy Protection Act)

Congress enacted the **Children's Online Privacy Protection Act (COPPA)** (15 U.S.C. 6501-6505) in 1998. It is enforced by the Federal Trade Commission (FTC).

The primary goal of COPPA is to allow parents to control what personal information is collected online from their children under age 13. The law applies to any vendors or operators of child-directed websites, online services including web-based testing, and programs or applications ("apps") that collect, use, or disclose children's personal information, whether at home or at school. Personal information can include a child's name, email, phone number, screen name, geolocation, photo, voice recording, or other persistent unique identifier. But it's important to note that COPPA only applies to personal information collected online directly from children; it does not cover information collected by adults that pertains to children. For more on COPPA, visit http://bit.ly/SPTK_COPPA [12]

Per the FTC, whether a website or online service is "directed to children" is determined by "subject matter of the site or service, its visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, or whether advertising promoting or appearing on the website or online service is directed to children."

What rights do parents have under COPPA?

If under-13 children use a website or app that fits the description above, the vendor or operator must obtain parental consent and provide clear and prominent notice of its use and disclosure practices on its website, including the following:

Per the FTC, COPPA "also applies to websites or online services that have actual knowledge that they are collecting personal information directly from users of ANOTHER website or online service directed to children."

1. THE NAME, address, telephone number, and email address of all other vendors or operators collecting or maintaining personal information through the site or service;

2. A DESCRIPTION of what personal information the vendor or operator is collecting, including whether the website or program enables children to make their personal information publicly available, how the vendor or operator uses such information, and the operator's disclosure practices for such information; and

Notice must be located on the "home or landing page or screen of its Web site or online service, and, at each area of the Web site or online service where personal information is collected from children."

3. NOTICE that upon request, parents can review and/or have deleted the child's personal information and refuse to permit its further collection or use, and a description of the procedures for doing so.

What rights do parents have under COPPA in schools?

1. SCHOOLS CAN CONSENT on behalf of parents to create accounts and enter students' personal information into online programs that children may then use in school or at home — whether for instruction, testing, or other purposes — but only where the vendor or operator of the online program collects personal information for the use and sole benefit of the school, and for no other commercial purpose. If the student's personal information is used for targeted ads, for example, or building user profiles for commercial purposes, the school CANNOT consent on behalf of the parent.

If a child-directed online program or website intends to use or disclose any personal information provided by under 13 students for its own or other commercial purposes, the school may not provide consent on behalf of parents.

2. WHEN SCHOOLS CONSENT on behalf of parents, COPPA transfers parental rights to the school. In this case, 1) a vendor or operator must provide the school — not parents — the clear and prominent notice of its use and disclosure practices on its website or elsewhere, as described above; and 2) schools — not parents — have the right to request that the vendor or operator delete students' personal information and cease further collection or use.

Before a school may consent to its students using online programs that collect personal information, the vendor of the website must provide the school with full notice of its how it collects, uses, and discloses student information.

If you believe a vendor or operator is in violation of COPPA, first notify your school, or district Superintendent. You may also contact your local chapter of the American Civil Liberties Union (ACLU) to request help; or contact the FTC to ask questions or file a complaint at https://www.ftccomplaintassistant.gov, email CoppaHotLine@ftc.gov or call toll free at (877) FTC-HELP.

Disclaimer: While the goal of the Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood is to provide valuable resources to help you protect student privacy, our suggestions should not be used in place of legal advice from an attorney. For questions on how federal, state, and local laws and policies may apply to your situation, you may wish to seek the advice of a licensed attorney by contacting your local bar association's referral service.

Questions? Visit www.studentprivacymatters.org/toolkit for more information, including free webinars on how to use the resources in this toolkit.

REFERENCES

1. https://nces.ed.gov/programs/slds/
2. https://ed.gov/policy/gen/guid/fpco/ferpa/index.html
3. http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf
4. https://www2.ed.gov/policy/gen/guid/ptac/pdf/idea-ferpa.pdf
5. https://www2.ed.gov/about/offices/list/osers/osep/osep-idea.html
6. https://www.fns.usda.gov/nslp/national-school-lunch-program-nslp
7. http://cjonline.com/news-education-local-state/2014-08-19/usd-501-admits-student-privacy-violations-says-breach
8. https://www.fns.usda.gov/sbp/school-breakfast-program-sbp
9. https://www.fns.usda.gov/smp/special-milk-program
10. https://www.fns.usda.gov/sfsp/summer-food-service-program
11. https://www.fns.usda.gov/cacfp/child-and-adult-care-food-program
12. https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

SECTION III.

Tips for parents looking to protect their student's privacy

Children and their parents are under intense pressure to engage with technology at home and at school. Whether children are voluntarily using personal social media or assigned to use applications (apps) and online programs by their teachers, they are sharing more and more details of their lives online. You may feel like the genie is out of the bottle, but it's not too late to take simple steps to protect your children's privacy. Give these suggestions a try!

Tips for home

RESIST THE URGE yourself to share everything with everyone. Before posting intimate photos or details about your children's life on social media, consider the long-term implications of sharing this information so widely. One study found that children resent their parents posting pictures of them on social media without their consent.[1] Another study found that the average parent in the United Kingdom shares nearly 1,500 photos of their children before they turn five.[2] Talking to your children about what's appropriate for you to post is also a great way to jump-start important conversations about their own social media behavior.

It's estimated that 81% of the U.S. population maintains at least one social network profile.[3]

SET BOUNDARIES with your children. Discuss what information is appropriate to share online and what is not. Encourage them to ask permission from their friends before posting or sharing pictures of their friends with others.

A recent study revealed that "[t]he same brain circuits that are activated by eating chocolate and winning money are activated when teenagers see large numbers of 'likes' on their own photos, and teenagers are definitely influenced by their online 'friends,' even if they barely know them."[4]

INSTALL AD-BLOCKERS on personal laptops, devices, and phones your children use at home. For example, Privacy Badger,[5] or a combination of AdBlock[6] and Ghostery,[7] allows websites to load faster and blocks ads that may contain malware or other viruses. These programs can also prevent companies from tracking and profiling your children.[8]

PLACE A STICKY NOTE or non-stick adhesive bandage (e.g., a Band-Aid) over the camera lens on your and your children's devices to prevent hackers from turning them on. Facebook founder Mark Zuckerberg and FBI Director James Comey do it![9]

BEFORE DOWNLOADING FREE APPS, consider that if an online service or product is ostensibly offered for "free," the real price you pay is often your children's information, to be exploited for marketing or other commercial purposes. Encourage your kids to ask your permission before signing up. If they're under age 13 and they are providing personal information, this is legally required under the Children's Online Privacy Protection Act (COPPA) when the website is child-directed. For more information on COPPA, see Section II.

Give yourself an added layer of protection by using the Electronic Frontier Foundation's "HTTPS Everywhere." Learn more at www.eff.org/https-everywhere

CONSIDER CREATING A NEW EMAIL ACCOUNT — with no real name or other identifying information attached — for signing your children up for apps or online accounts.

TEACH YOUR CHILDREN to create usernames and passwords for online accounts

without using any of their personal identifying information like their names, dates of birth, student number, pet name, or school names.

Help your child create strong passwords! Try using an acronym for something your child will easily remember, preferably a full sentence. Use combinations of upper- and lower-case letters, numbers and symbols. For example, the sentence "I love the FIFA World Cup video game" could be expressed as "I<3tFIFAWCvg."

TERMS OF SERVICE and privacy policies are often deliberately long, complicated, and hard to understand. Use the section below, What to look for in terms of service and privacy policies, to scan the policies and terms of any apps or online programs used by your children. If you see any of the red flags from that list, do not allow your child to use them.

Tips for school

ASK YOUR CHILDREN'S TEACHERS which classroom apps and online programs will be assigned throughout the year, and what personal student information each app collects. Ask if these programs have been approved by either the district or state for privacy and security protections and compliance with state and federal laws. For a list of questions to ask your teacher, see Section V and Appendix D.

Education technology is big business! In February 2015, the Software and Information Industry Association (SIIA) estimated the value of the PreK-12 educational software and digital content market at $8.38 billion.[10]

ENCOURAGE YOUR CHILDREN'S TEACHERS and school to resist using non-essential classroom apps and online programs whenever possible. Consider opting your children out of using insecure or excessive apps and online programs.

ASK YOUR CHILDREN'S TEACHERS if they can create accounts without using their students' real names, and/or refrain from disclosing any student information not needed for the use the app or online program.

Why are some classroom apps free and what does this mean for your child's privacy? Technology can be a tool to enhance student learning, but it can also be expensive, which is why free software and classroom apps are so appealing to schools and teachers. But as the old saying goes, "nothing in life is free." If the school or district is not paying for the classroom app or online program, the company is most likely profiting from your child's information in some other way.

DON'T ASSUME the privacy policies of apps or online programs assigned to your children — especially free ones — have been sufficiently vetted by their teachers. Educational or classroom apps may not respect student privacy any more than other apps.

SCAN THE TERMS OF SERVICE and privacy policies of any classroom app or online program your children are assigned. If you see any of the red flags described in the section below, approach the teacher or principal with your concerns.

ASK YOUR PRINCIPAL if the school keeps personal student information in the "cloud," and if so, if there is a contract to bar the vendor or operator from selling the information, redisclosing it to others, or using it for non-educational purposes. Ask if the information is properly encrypted in transmission and at rest.

A 2010 study by Fordham Law School found that "95% of districts rely on vendors for a diverse range of functions including data collection and mining related to student performance, support for classroom activities, student guidance, data hosting, as well as special services such as cafeteria payments and transportation planning."[11]

TALK TO YOUR HIGH SCHOOL CHILDREN about military recruiters who may be visiting their school campus. If your children are not considering enlisting in the military, make certain they do not accept gifts offered by recruiters or share any personal information with them.

SUBMIT A WRITTEN REQUEST to your principal to opt out of providing your high school children's personal information to military recruiters. See Appendix C for a sample form.

ASK YOUR PRINCIPAL how to opt out of "directory information" to prohibit the school from sharing personal information with some third-parties as is your right under the Federal Education Rights and Privacy Act or FERPA. Your school should provide you these

forms without being asked, but many don't. Also, schools often have a deadline to opt out of directory information disclosure, typically within the first ten to thirty days of a school year. For more on this, see Section II and Appendix B for a sample directory information opt out form.

EXERCISE YOUR RIGHTS under FERPA to access and review your children's educational records at the school and district level each year, as well as records contained in the statewide longitudinal data system (SLDS). Ask to correct any mistakes you see in these records. For more information about the SLDS, see Sections II and VII. To request access and review your child's records, use the sample request form in Appendix A.

WHEN REGISTERING YOUR CHILDREN for College Board's PSAT/SAT or ACT exams, do not check the box to opt into sharing extraneous personal information with colleges or other organizations, and do not provide these companies with any unnecessary information. Your children may also be asked to provide personal information again on exam day; they should be discouraged from checking the box or providing anything other than name, grade, school, and other details required to take the test. When students fill in this additional information, the data is often sold by the testing companies to colleges and others, to be used for marketing and recruitment, or to help colleges decide who to accept or reject.

Prior to the test, your child's teacher may read aloud instructions prepared by the College Board/ACT that may make it sound to students as if they are required to answer personal questions. Make sure you inform your child before the test that providing answers to any questions touching on the subjects below is strictly voluntary.

Questions may touch on the following sensitive subjects:
- *contact information;*
- *major;*
- *gender;*
- *disability status;*
- *grades and rank;*
- *ethnicity;*
- *religion;*
- *educational aspirations;*
- *parent income and financial aid;*
- *sports;*
- *college living preferences;*
- *citizenship;*
- *ROTC;*
- *desired college characteristics;*
- *high school courses and activities; and*
- *honors.*

What to look for in terms of service and privacy policies

If the terms of service and/or privacy policies of online programs your children use at home or school include any of the red flags below, consider not using the programs. The language should be reviewed by an attorney or school official to ensure they are not in violation of federal or state laws or district policies.

EXAMPLE: "The Company reserves the right, at its sole discretion, to modify or replace any part of this Privacy Policy."

REASON FOR CONCERN: Companies should not be allowed to change their policies without first notifying and obtaining consent from users. In the case of apps used at schools, unilateral changes made by a company may result in inappropriate or even illegal disclosure or use of student information.

For additional examples, refer to the U.S. Department of Education's Privacy Technical Assistance Center at http://ptac.ed.gov/

EXAMPLE: "By using the Service, you are authorizing the Company to use, gather, parse, and retain any data related to the delivery of the Service."

REASON FOR CONCERN: Companies should be very explicit about what user data they collect, and how it will be used, shared, and deleted. When apps are used in schools, they are generally allowed to use student information for educational purposes only. To use it for any other purpose — commercial or otherwise — may be a violation of federal law, including FERPA and COPPA.

EXAMPLE: "The Company shares your information with third-party business partners for the purpose of providing the Service to you. We may also share certain information such as browser and cookie data and other data relating to your use of our Service with our business partners to deliver information about products or services that may be of interest to you."

REASON FOR CONCERN: Companies should identify by name, address, phone number, and email address any other third parties collecting or maintaining your children's personal information gathered through the app. If not, they may be in violation of COPPA (if your child is under 13 and the website is child-directed) or FERPA. Additionally, companies should not use information collected about children to develop marketing profiles or serve ads to children or their parents.

EXAMPLE: "The Company and its partners and licensors may collect, use, transmit, process and maintain your location data, including but not limited to the geographic location of your device (e.g., latitude and/or longitude) and information related to your account."

REASON FOR CONCERN: Whether the app is used at home or school, companies should not collect children's geographic location data.

EXAMPLE: "No data transmission over the Internet is 100% secure. The Company will strive to protect your personally-identifying information, but we cannot warrant the security of any information you transmit to us and you do so at your own risk."

REASON FOR CONCERN: Companies should always encrypt users' personal data, employ other best practices to secure data, and should not try to exempt themselves from liability if breaches occur.

CommonSense Media advises parents to "look for the 'https' in the URL" and offers other tips to enhance student data privacy and security at https://www.commonsense.org/education/privacy

Their December 2016 survey revealed that 25 percent of education technology websites did not support encryption, and 20 percent did not require an encrypted connection.[12]

EXAMPLE: "The Company may share information that we collect in connection with a corporate transaction, such as the sale of our services, a merger, consolidation, asset sale or in the event of bankruptcy."

REASON FOR CONCERN: While some state privacy laws ban the sale of personal student data, companies may claim exceptions to allow for the sale of the data in case of a merger, bankruptcy or "asset" sale. Others may claim that they while they will not sell the data, they may "license" it for a fee to other companies or organizations. Parents should be wary of such statements in a corporate terms of service or privacy policy.

Disclaimer: While the goal of the Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood is to provide valuable resources to help you protect student privacy, our suggestions should not be used in place of legal advice from an attorney. For questions on how federal, state, and local laws and policies may apply to your situation, you may wish to seek the advice of a licensed attorney by contacting your local bar association's referral service.

Questions? Visit www.studentprivacymatters.org/toolkit for more information, including free webinars on how to use the resources in this toolkit.

REFERENCES

1. http://well.blogs.nytimes.com/2016/03/08/dont-post-about-me-on-social-media-children-say/?_r=0

2. http://www.nominet.uk/wp-content/uploads/2016/09/Nominet-Share-with-Care-2016-Infographic.pdf

3. http://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/

4. https://www.sciencedaily.com/releases/2016/05/160531104423.htm

5. https://www.eff.org/privacybadger

6. https://getadblock.com/

7. https://www.ghostery.com/

8. http://www.computerworld.com/article/2692560/six-browser-plug-ins-that-protect-your-privacy.html

9. http://www.nytimes.com/2016/06/23/technology/personaltech/mark-zuckerberg-covers-his-laptop-camera-you-should-consider-it-too.html?_r=0

10. http://www.siia.net/Press/SIIA-Estimates-838-Billion-Dollars-US-Market-for-PreK-12-Educational-Software-and-Digital-Content

11. http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip

12. https://www.commonsense.org/education/privacy/survey/encryption

SECTION IV.

Student privacy best practices for states, districts, schools, and teachers

In an ideal world, sensitive student information would be held under lock and key and shared only with parental permission to trusted teachers, counselors, tutors, and other school staff. While this may not be possible in today's data- and technology-driven schools, it is important to implement thoughtful best practices to safeguard student information at the state, district, and school level.

These recommendations come from our coalition's Five Principals to Protect Student Privacy,[1] the U.S. Department of Education's Privacy Technical Assistance Center (PTAC),[2] and other expert organizations concerned with this issue. Though our best practices may go beyond what's required in current federal and state law, states, districts, schools and their teachers should implement these policies if they want to improve student privacy and security protections and limit their own liability. Share these with your school today!

THE IMPORTANCE OF WRITTEN AGREEMENTS

One of the best methods to help protect student information is to require written agreements, contracts, or memoranda of understanding (MOUs) between states/schools/districts and any third parties accessing or receiving personal student information, including companies who offer online instructional programs or free classroom applications (apps). Written agreements can limit how student information is collected, used, and shared with others; they can also require the company to adopt strong security and breach notification requirements, include enforceable penalties for noncompliance, and enumerate recourse procedures for parents. For a complete list of what should be included in written agreements, see the Consortium of School Network's (CoSN) document titled "Suggested Contract Terms," (http://bit.ly/SPTK_COSN)[3] and a sample contract prepared by the Massachusetts Student Privacy Alliance (http://bit.ly/SPTK_MSPA).[4]

Note: If states, schools and/or districts share student information with organizations and agencies without parental consent as allowed under the FERPA "studies" or "audit or evaluation" exceptions, as described in Section II, a written agreement is required. See the "Written Agreement Checklist" (http://bit.ly/SPTK_WAC)[5] provided by the U.S. Department of Education Privacy Technical Assistance Center for more information.

Best practices for state education departments

REQUIRE written agreements, contracts, or MOUs between the state and any third parties receiving personal student information, and post them prominently on the state's website.

APPOINT a Chief Privacy Officer who is an expert in the law and privacy and security practices to be responsible for establishing a comprehensive data governance program and communicating with parents who have questions or concerns.

CREATE a data stakeholder advisory council that includes parents, teachers, and privacy experts to provide input and oversee student data collection, governance, and disclosure.

The U. S. Department of Education Privacy Technical Assistance Center recommends that data governance programs should address:
"• protection of sensitive data;
• vulnerability assessment and risk management;
• enforcement of legal, regulatory, contractual, and architectural compliance requirements;
• identification of stakeholders, such as parents and administrators, their roles and responsibilities; and
• access management."

This is critical to ensure that privacy and security are prioritized and that the public has input into decisions pertaining to the use of student personal information.

ASSESS online instructional programs and free classroom apps for their educational content and purpose, data use practices, and privacy and security standards, and approve or reject them accordingly. No online programs or apps should be considered for use from any vendors or operators that have not signed a contract with the state and agreed to the Student Privacy Pledge, [6] which bans the sale of personal student information except in the case of mergers, acquisitions, and bankruptcies. Signers of the Student Privacy Pledge also commit to not using student information "for behavioral targeting of advertisements to students."

Best practices for school districts and schools

REQUIRE written agreements, contracts, or MOUs between the district/school and any third parties accessing or receiving personal student information. Post them prominently on the school or district website and contact parents directly with information about where to read them.

The Consortium of School Networks (CoSN) recommends that contracts should: "Include a specific restriction on the use of student information by the provider for advertising or marketing purposes or the sale or disclosure of student information by providers."[7]

Fordham Law School recommends that "cloud service agreements" should: "Include a clause explicitly addressing the sale and marketing of transferred data or the use of that data by the vendor itself for sale and marketing purposes without parental consent."[8]

ADOPT and adhere to the state education department's approved list of online programs and apps, and post the current list on the district or school website. Districts may also choose to create an even more rigorous procedure for vetting online programs and apps.

DESIGNATE a Chief Privacy Officer or someone on staff responsible for ensuring best practices and communicating with parents.

WORK WITH parents, teachers, and privacy advocates to adopt transparent policies around the collection, use, and protection of student data, including:

- Identifying and then minimizing the collection of personal student information;
- Justifying the purpose for each type of collection, including an explanation of its educational purpose;
- Describing how the information is collected, stored, and protected from breaches, and how parents can access and, if necessary, correct it;
- Identifying to whom the information will be disclosed (including individuals, organizations, or vendors or operators outside the school or district) and for what purposes; and
- Defining the process for notifying parents before information is disclosed.

We recommend that notification to parents should include:
• A list of the classroom apps and online programs students are required or encouraged to use.
• The educational purpose or value of each app or online program.
• Student data that each app or online program will collect.
• Key provisions of each app or online program's privacy policy.
• Whether parents can opt out of their children's use of the apps or online programs, and if so, what alternatives will be provided.
• Whether an app or online program collects and analyzes data to create a learning profile that will direct a student's lessons or educational pathways. If it does, parents should have the technology explained to them and a way to challenge its accuracy and utility.

PROHIBIT schools from disclosing any personal student data, including "directory information," to any third parties who intend to sell or use student information for marketing purposes.

ADOPT a policy allowing parents to specify which "directory information" can be shared and with which third parties. For more information, see Section II.

ASK FOR parent permission or consent before sharing highly sensitive data such as disability, health, and disciplinary data with third parties, including vendors, operators, or other organizations.

■ PROVIDE regular data security training, including best practices, to teachers, administrators, and anyone who handles personal student data.

Fordham Law School recommends: "For larger districts and those with extensive cloud networks and intensive data transfers, the designation of a chief privacy officer with responsibility for data governance, privacy compliance, and teacher training is necessary to assure proper stewardship of student data and to enable those districts to more effectively assure the protection of their students' information."

■ PROHIBIT teachers from assigning or encouraging students to use any classroom apps or online programs not on the state or district approved list.

■ PROHIBIT "data walls" displaying a student's personal information, including names or other identifying information, from being posted in any semi-public areas, including classrooms or hallways.

Best practices for teachers

■ BEFORE ASSIGNING an online program or classroom app, consider whether its use is necessary — many privacy issues can be avoided by simply not adopting every new online tool marketed to schools.

The U. S. Department of Education Privacy Technical Assistance Center recommends that schools and districts "[h]ave policies and procedures to evaluate and approve proposed online educational services."

■ DO NOT USE or ask students to use any online program or app unless it has first been vetted and approved by your state education department or district.

■ BE PREPARED to offer an appropriate alternative (e.g., a textbook or paper and pencil version) to students whose parents choose to opt out of an online program that accesses their personal information.

Houston Independent School District developed a system to evaluate the privacy, safety, and security of commonly used Web Apps. You can check out the criteria used to rate them here: http://www.houstonisd.org/Page/126147

■ NEVER SIGN UP for online programs or classroom apps with "click-wrap" agreements — when a user checks a box to accept terms and conditions before using a product or service — unless the terms have been rigorously reviewed by someone with legal and/or technical expertise. Remember that even with review, the terms of service may change over time, putting students' privacy at risk. To learn more about click-wrap agreements, see PTAC's guidance at http://bit.ly/SPTK_PTAC [9]

■ EDUCATE YOURSELF in the principles of good digital citizenship and incorporate responsible technology practices in your classroom. Incorporate Fordham Law School's "Privacy Educators Classroom" curriculum into your lessons, found at https://www.fordham.edu/info/24071/privacy_education.

Sign up today for privacy trainings offered by the U.S. Department of Education at http://ptac.ed.gov/

■ WHEN CREATING "data walls" that display students' test scores or grades in public areas like classrooms or hallways, never include any information that could be used to identify them.

Disclaimer: While the goal of the Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood is to provide valuable resources to help you protect student privacy, our suggestions should not be used in place of legal advice from an attorney. For questions on how federal, state, and local laws and policies may apply to your situation, you may wish to seek the advice of a licensed attorney by contacting your local bar association's referral service.

Questions? Visit www.studentprivacymatters.org/toolkit for more information, including free webinars on how to use the resources in this toolkit.

REFERENCES

1. http://www.studentprivacymatters.org/five-principles-to-protect-study-privacy/

2. http://ptac.ed.gov/

3. http://www.cosn.org/sites/default/files/pdf/Suggested_Contract_Terms_09_2014.pdf

4. https://secure2.cpsd.us/mspa/MSPA_Student_Data_Privacy_Agreement_V4.pdf

5. http://ptac.ed.gov/sites/default/files/Written_Agreement_Checklist.pdf

6. https://studentprivacypledge.org/

7. http://cosn.org/sites/default/files/CoSN-Privacy-Toolkit.pdf

8. http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip

9. http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf

SECTION V.

Talking to teachers, schools, and districts about student privacy

You don't have to be an expert on privacy law or district policies to raise concerns about student privacy. Simply schedule an appointment with your child's teacher or principal and ask some questions to help open the lines of communication. Here are some suggested questions; you do not need to ask them all. You can also follow up with some of the additional questions in Appendix D.

- APPROXIMATELY HOW MANY HOURS PER DAY will my child be expected to use an electronic device, including computers, laptops, tablets, and/or smartphones?
- WHAT ONLINE PROGRAMS and classroom applications (apps) will my child be assigned to use in class this year?
- HAVE THESE PROGRAMS and apps been vetted for data privacy, security, and compliance with state and federal privacy laws?
- WHAT DATA IS COLLECTED about my child by the school, its contractors, and any vendors, or operators of online programs and apps used in classrooms?
- WHICH OF THIS DATA is being sent to the state department of education?
- ARE THE VENDORS supplying these programs barred from using the data for marketing purposes and sharing it with other third parties, and/or subjecting my child to ads?
- HOW CAN I ACCESS the data for my child collected and stored by the vendor or operator, the school, the district, or the state? (See Section II for more information on your rights to access this information under federal law.)
- WHO ON THE SCHOOL STAFF and among school contractors, vendors, or operators has access to my child's data?
- WHAT IS THE POLICY, if any, governing who may access my child's data and under what circumstances?
- HOW IS MY CHILD'S DATA protected against security breaches?
- HOW LONG do the school, contractors, or vendors or operators of online programs and classroom apps retain my child's data?
- WHAT DATA does the school or device provider (e.g., Microsoft, Apple, Google, etc.) have access to when my child is using a school-provided device? For example, can the school or device provider access:
  - location information;
  - IP addresses;
  - camera and microphone;
  - browsing history;
  - locally stored content;
  - contacts; or
  - anything else not explicitly provided to the school by my child?
- DOES THE SCHOOL offer a way for families to opt out of or minimize the amount of data collected by the school or any online programs/classroom apps used in class?
- WHO ELSE can I ask if you can't answer my questions?

These suggestions are adapted from the WICKR Foundation at www.wickr.org/expiration-date-for-kids-data/

Questions? Visit www.studentprivacymatters.org/toolkit for more information, including free webinars on how to use the resources in this toolkit.

SECTION VI.

Advocating for student privacy in schools, districts, and beyond

If you're dissatisfied with your school's response to your questions and concerns outlined in Section V, it may be time to advocate for better privacy practices and policies. You can do this! It helps to connect with other parents in your school community who are similarly concerned. You may also find allies and experts in other organizations who can provide you with valuable information and support.

Important first steps

- TALK TO OTHER PARENTS in your child's class and/or parent-teacher organization members to share your concerns.
- PREPARE REMARKS and speak before your school board; ask a friend to videotape your presentation and consider posting it online.
- TOGETHER WITH OTHER PARENTS, post an online petition or collect signatures on a petition outside the school; be sure to collect emails and other contact information. For a sample petition asking a local school board for public hearings to address student privacy issues, see Appendix E.
- IF YOU USE SOCIAL MEDIA, post your concerns on your personal account, or a relevant account from your local community. You can also set up your own social media account specifically concerned with the issue. Social media can be a powerful tool!
- FOLLOW UP with your district administrators or school board members, and/or local elected officials who represent you, and seek a meeting that includes other parents who share your concerns.

Try these three conversation starters:

1. "My child seems to be taught more and more by computer programs rather than the teacher. Have you noticed this?"

2. "I can't keep track of all the accounts and logins my child must remember to complete her homework. Is your family also overwhelmed?"

3. "I remember the old days when we spoke to our children's teachers face to face rather than thorough notifications on our phone. Do you find this kind of impersonal too?"

Organize, engage, and empower

- ONCE YOU'VE IDENTIFIED a small group of active parents with the same concerns, hold a meeting at a community center, library, church, or other gathering space.
- INVITE EXPERTS sympathetic and knowledgeable on the issue, such as members of your local American Civil Liberties Union (ACLU), local elected officials, or Information Technology (IT) specialists, to speak on the topic of student privacy and answer questions. Parents can describe how lax student privacy practices may have affected their own children or put their privacy at risk.
- INVITE MEMBERS of the school community through social media, email, and flyers. Be sure to invite parents who signed your petition.

When preparing remarks, a good place to start is by using or modifying our suggestions in Section IV.

DECIDE if you want to ask local media to publicize the meeting, and/or invite reporters to attend who can help spread the word. More on how to do this below.

PRESENT INFORMATION from our toolkit, including Section IV.

AFTER A QUESTION AND ANSWER PERIOD, discuss collectively or in smaller groups what your next steps will be. Be sure to pass out information about your petition along with your contact information.

If you have a meeting or presentation, you can copy and include any section or handout from this toolkit – use whichever is most relevant to what you are trying to achieve.

Expand your reach

ARRANGE a follow up meeting with district administrators, school board members, or local elected officials to discuss your concerns and present your petition.

ASK ADMINISTRATORS to consider adopting best practices to secure and protect student information. You can use our recommendations in Section IV as a starting point.

URGE SCHOOL BOARD MEMBERS to sponsor a resolution to adopt these suggestions.

ASK LOCAL ELECTED OFFICIALS to write a letter of support.

Reach out to helpful groups[1] who are concerned about student privacy:

Parent Coalition for Student Privacy
Campaign for a Commercial-Free Childhood
Electronic Frontier Foundation
Network for Public Education
Electronic Privacy Information Center
Parents Across America
American Civil Liberties Union

DON'T FORGET!

Be sure to follow-up any meeting with a letter thanking officials for their time and holding them accountable for any promises they may have made. If they are not prepared to support improvements in protecting student privacy, ask them to justify why not. Share any responses, whether positive or negative, more broadly with concerned parents and with reporters.

Get media attention

If you're organizing a town hall meeting, rally, or protest, or simply advocating on an issue, gaining media attention is extremely useful to achieving your goal.

IF YOU'RE HOLDING an event, send a brief press advisory in the body of an email to reporters a week before and a reminder again the day before the event, no later than 2 PM. Include the date of the event in the subject line, telling where, when, and what. Be sure to add a contact person with email and phone number for more information. See Appendix F for a sample with helpful hints that you can use to write your own advisory.

Do not overuse your press email list or reporters will start treating your messages as spam.

Email the press advisory (with no attachments) to the Associated Press at info@ap.org, and contact the appropriate regional desks listed here to find out where you should send it through email or fax: http://www.ap.org/contact-us/bureaus

AT THE EVENT, ask a friend to take photos and/or video, and post them online to your social media accounts and to YouTube, Facebook, Twitter, Flickr, etc. Make it clear to participants ahead of time that you are recording and may be sharing this event more widely with members of the public, and allow speakers to opt out of being recorded if they prefer.

Pick quotes and soundbites that are clear, simple, catchy, powerful, emotional, and add value to the story.

DISTRIBUTE A PRESS RELEASE after the event to reporters. The release should be a one- or two-page document that briefly describes the event, the participants, and the issue discussed. If you can, include quotes and soundbites. See Appendix F for a sample with helpful hints that you can use to write your own release.

SEND THE PRESS RELEASE after the event to reporters, parents, officials, and others who could not attend.

IN GENERAL, it's important get to know your local reporters so you can piggyback on any breaking news that relates to student privacy. Jumping on a news story is the best way to draw more attention to the issue and your point of view. Prepare a good soundbite in advance that sums up your perspective in a few words or sentences. Once a reporter knows you're interested in the subject, they may contact you looking for a relevant quote the next time the issue arises.

WRITE LETTERS to the editor; do not forget community papers.

TIPS FOR WRITING A LETTER TO THE EDITOR:

1. Most published letters to the editor are in response to a topic recently covered in the publication, so keep an eye out for stories related to student privacy, including breaches.
2. When you find a story, research the submission rules of the specific publication. Many limit the number of words to 200-250 so keep the letter short.
3. Introduce yourself and explain why the issue concerns you. Follow with a compelling statement including facts or details. Letters with local relevance may have a better chance at getting published.
4. Make your point by including information important to readers of the publication and conclude with a call to action (e.g., sign my petition).
5. Don't forget to sign your letter with your first and last name, and provide your email address and telephone number.

For more tips, see the International Society for Technology in Education advocacy toolkit at http://bit.ly/SPTK_OpEds [2]

And be sure to contact the Parent Coalition for Student Privacy at info@studentprivacymatters.org. We may be able to help!

Questions? Visit www.studentprivacymatters.org/toolkit for more information, including free webinars on how to use the resources in this toolkit.

REFERENCES

1. http://www.studentprivacymatters.org/

   http://www.commercialfreechildhood.org/

   https://www.eff.org/

   http://networkforpubliceducation.org/

   https://epic.org/

   http://parentsacrossamerica.org/

   https://www.aclu.org/

2. http://www.iste.org/docs/pdfs/iste-advocacy-toolkit---letter-to-the-editor.pdf

SECTION VII.
Student privacy FAQs

Here are some answers to commonly asked questions about student privacy. We urge parents to consult the entire toolkit for more information. If you can't find what you're looking for, email us at info@studentprivacymatters.org. We'll do our best to find answers to your questions!

Q: What is FERPA and what records does it protect?

A: The Federal Education Rights and Privacy Act (FERPA) was enacted in 1974 to protect the privacy of "education records" of students in schools and universities that receive federal funds. Education records are defined as those that are "(1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution." For more information, see Section II.

Q: Under what circumstances can the contents of my child's education record be shared without parental consent?

A: FERPA has been relaxed through regulation in recent years, allowing schools to disclose personal information in your child's education record to third parties under a variety of conditions. For an explanation of these circumstances, see Section II.

Q: Can my child's personal information be shared with every employee within the school?

A: No. A student's personal information can be shared only with those members of the school staff directly responsible for his or her education or services, and only as much information as necessary for them to fulfill their professional duties.

Q: Can my school or district share my child's information with the state education department without parental consent?

A. Yes. Most schools and/or districts report student-level information with the state department of education on a regular basis; some of this data may be required to meet accountability provisions outlined in federal or state law. Other data collection may be purely discretionary on the part of the state. Student information sent by schools to the state is typically stored in the statewide longitudinal data system (SLDS) and may be linked with data from other state agencies, including health and human services, higher education, labor, corrections, and public safety. Information held in the SLDS may then be made available to researchers and policymakers if the state decides to do so. Nearly every state in the nation has an SLDS; the goal of the SLDS program is to track students from preschool through high school, college, and beyond.

WHAT STUDENT DATA IS IN YOUR STATE'S SLDS?

Every state in the nation, except Wyoming, New Mexico, and Alabama, received federal grant funding from the U.S. Department of Education to develop or maintain an SLDS. States that received funds were required to adopt the following minimum requirements for their data systems:

1. A unique identifier for every student that does not permit a student to be individually identified (except as permitted by federal and state law);
2. The school enrollment history, demographic characteristics, and program participation record of every student;
3. Information on when a student enrolls, transfers, drops out, or graduates from a school;

4. Students' scores on state tests as required by the Elementary and Secondary Education Act;
5. Information on students who are not tested, by grade and subject;
6. Students' scores on tests measuring whether they're ready for college;
7. A way to identify teachers and to match teachers to their students;
8. Information from students' transcripts, specifically courses taken and grades earned;
9. Data on students' success in college, including whether they enrolled in remedial courses;
10. Data on whether K-12 students are prepared to succeed in college;
11. A system of auditing data for quality, validity, and reliability; and
12. The ability to share data from preschool through postsecondary education data systems.

NOTE: Many state SLDS contain information specifically identifying students including names, addresses, disability diagnoses, and even suspension details.

Find out how much federal grant funding your state received to develop or maintain a statewide longitudinal data system (SLDS) at http://bit.ly/SPTK_SLDS [1] and learn details about your state's SLDS at http://www.workforcedqc.org/state-solutions

Q: Can I access information in my child's education record? What should I do if it is inaccurate?

A: Yes. FERPA guarantees parents the opportunity to inspect and review your child's education records within 45 days upon request, whether they are held by the school, the district, or the state. You cannot be charged a fee for the school or education agency to search or retrieve these records, but a minimum fee may be charged to make copies. FERPA also gives you the right to correct information in your child's records if you believe it is "inaccurate, misleading, or in violation of the privacy rights of the student." For more information about your rights to access and correct or challenge information in an education record, see Section II.

Q: Is my child's medical information included in her/his education record? Is it protected by HIPAA (the Health Insurance Portability and Accountability Act)?

A: In most cases, medical information that you or your child provides to the school, as well as records made by a school nurse, counselor, or school-operated health clinic, become part of the education record and are covered by FERPA, not HIPAA. The disability and support services that a special education student receives are also part of their education record, and can be disclosed without parental consent under the conditions or exceptions noted in Section II.

Generally speaking, schools are not required to comply with HIPAA because they are not considered "covered entities" under the law, such as health plans, health care clearinghouses, and health care providers. Regardless, you should ask your school who has access to your child's medical, disability or counseling records, and advocate for this information to be closely held within the school and for its disclosure outside the school to be limited as much as possible. To learn more about HIPAA in schools, please visit http://bit.ly/SPTK_HIPAA [2]

Q: If I email my child's teacher about a confidential issue, will that information be included in my child's education record?

A: It could be. If you have a sensitive matter you want to discuss with your child's teacher, we suggest scheduling a private face-to-face meeting to discuss your concerns. Anything written that you share—handwritten notes or email communication—could become part of your child's education record.

Q: Is my child's digital information collected by classroom applications (apps) or online programs protected by FERPA?

A: It depends on many factors including, but not limited to, what student information the classroom app or online program collects and/or maintains, and how it uses and shares the information. FERPA became law in 1974, long before technology became so pervasive in our classrooms. While the U.S. Department of Education Privacy Technical Assistance Center (PTAC) has attempted to provide some guidance on this issue, schools and districts are advised to evaluate on a "case-by case basis" whether FERPA applies. Until federal law is updated and strengthened to protect all student information—digital or otherwise—we offer important recommendations you can share with your school, district, and/or state in Section IV.

Q: My child's teacher or principal told me a classroom app or online program used in my school is FERPA compliant. What does this mean?

A: This statement should not reassure you that your child's information is kept private or is well-protected. FERPA allows for broad disclosures of personal information contained in student records without parental consent, as described in Section II, and the law requires no minimum standards for data security protections. Additionally, FERPA regulates the practices of schools that receive federal funds; it does not directly regulate the actions of private vendors or online operators. If a vendor or operator uses student information for an unauthorized purpose, parents should hold local education officials accountable to maintain strict oversight and stop the practice. For more information on best practices, please refer to Section IV.

Q: What is the punishment for a FERPA violation?

A. If a school is found in violation of FERPA, federal funding may be withheld. However, the federal government has never done this in FERPA's 43-year history. Additionally, certain third parties may be banned by the U.S. Department of Education from receiving student's personal information for up to five years if the party re-disclosed student data in violation of FERPA. If an organization fails to destroy student information after it's no longer needed for purposes of a "study," it may also be banned from receiving student information for up to five years.

Q: Is my child's teacher allowed by law to sign up my child for classroom apps or online programs without my permission?

A: Under the "school official" exception, FERPA allows your teacher to use personal information from your child's education record to create an online account without your consent. This may also be done with a more limited set of student information using the "directory information" exception. However, if your child is under the age of 13 and is entering personal information into a child-directed online program himself, either at school or at home, the federal Children's Online Privacy Protection Act (COPPA) would apply. A teacher may consent to your child's use of an online educational tool if any personal information collected by the online vendor or operator is not used for any commercial purpose. It is the responsibility of the school, district, or state to ensure that the vendor or operator uses student information only for specified purposes and secures it sufficiently. As noted in Section IV, we recommend that no teacher should sign up students to online programs without a careful vetting of the program at the school, district, or state level.

MORE INFORMATION ON COPPA IN SCHOOLS

For a teacher/school to provide consent on behalf of a parent, the operator of the classroom app or online program must provide the school with all the notices required under COPPA.

Additionally, upon request by the school, the operator must provide the school:

1. A description of the types of personal information collected on students;
2. An opportunity to review the student's personal information and/or have the information deleted; and
3. The opportunity to prevent further use or online collection of a child's personal information.

For more information about parent's rights under COPPA, see Section II.

Q: Can personal student information be sold by schools or the companies they allow to collect it? Can it be used to target advertisements to students?

A: Many state laws, including California's 2014 landmark Student Online Personal Information Protection Act (SOPIPA), prohibit companies that collect data through their online educational services from selling student information — except when a vendor or operator's company is acquired by another company, in which case the new vendor or operator must comply with all privacy provisions in the law. SOPIPA and some other state laws also prohibit the use of personal student data for targeted advertising.[3]

FERPA prohibits companies designated as "school officials" from using student data for any reason other than the purpose originally authorized, unless a parent or eligible student has provided consent for an additional purpose. That is, unless the school has authorized a company to use student data for targeted ads, supposedly for educational purposes, or the parent or eligible student consents, the company may not do so. However, FERPA does allow the disclosure of "directory information" without limitations, including marketing to students and selling the information to others. For more on directory information and how to opt out of its disclosure, see Section II.

COPPA prevents vendors or operators of child-directed websites or apps from using personal information that is collected directly from a student under the age of 13 for commercial purposes, such as marketing or sharing the information with other companies for that purpose, unless a parent provides consent.

The Protection of Pupil Rights Amendment (PPRA) requires schools to notify parents and allow them to opt-out when students are "scheduled to participate in activities involving the collection, disclosure, or use of personal information collected from students for marketing purposes, or to sell or otherwise provide that information to others for marketing purposes." However, PPRA does allow companies, vendors, and operators to use students' personal information for the "exclusive purpose of developing, evaluating, or providing educational products or services for students or schools."

Q: Do companies offering college entrance exams, e.g., the College Board (PSAT/SAT) and ACT, sell information my child provides voluntarily?

A: Yes. You may have noticed a check box as part of the PSAT, SAT or ACT online registration form asking you or your child to opt in to sharing his or her information with colleges and scholarship programs. On each exam day, your child may also be encouraged to check the same box and provide more information. If you or your child opt in, your child's personal profile may then be sold to eligible colleges or other organizations for marketing or admissions decisions. To protect your child's privacy, we recommend that no extraneous personal information be provided to the College Board or ACT by either you or your child.

NOTE: If you've already opted-in to sharing your child's information through the College Board (SAT) Student Search Service, it is possible to revoke your permission by visiting: https://student.collegeboard.org/student-search-service/opt-out

Q: My child told me she/he took a survey at school which asked very personal questions. Is this allowed?

A: Under the PPRA, written parental consent must be obtained before a child can be asked to take a federally-funded survey, analysis, or evaluation that asks questions related to political affiliations, religious beliefs, sexual behavior and attitudes, and other sensitive

issues. If the survey asks questions about these types of personal issues but is not federally funded, parents must be notified in advance and be allowed to opt their children out of taking the survey. For more on PPRA and the type of questions it regulates see Section II.

Q: Does the school have an obligation to inform parents when there is a breach of student data?

A: None of the federal student privacy laws (FERPA, COPPA, PPRA) require schools to inform parents when student information has been breached. However, some state laws require this notification. In addition, FERPA requires that schools maintain in your child's education record an additional record of any unauthorized disclosures such as a data breach, and must make that information available to parents upon request. For more information, see Section II. As incidents of data breach in education are on the rise, we urge parents to advocate for stronger breach disclosure rules at the school, district, and state levels.

Q: Is it true that military recruiters can obtain my high school child's personal information directly from the school? Can I refuse to allow the school to provide it?

A: Yes. Under Section 9528 of No Child Left Behind (NCLB) and under Section 8025 of the Every Student Succeeds Act (ESSA), military recruiters may request access to the contact information of students. Parents can opt out of this disclosure by submitting a written refusal form to the school or district; see Appendix C for a sample form.

Q: What are "data walls," and under what circumstances are they prohibited?

A: Data walls are charts that teachers use to display students' test scores and/or progress in a subject or skill. FERPA generally prohibits the disclosure of such personal student information to non-school officials without the consent of the parent. If the information on a data wall includes your child's name or other identifying information, such as student ID, along with grades or test scores, is visible to any non-school employee in a semi-public area such as a classroom or hallway, and was posted without your consent, this violates FERPA.

HOW CAN DATA WALLS CONTRIBUTE TO STEREOTYPING?

Prior to the start of school, teachers may view details from a student's academic file, including grades, attendance, exam scores, and disciplinary records via a data wall or through an online interface called a data dashboard. Students with positive histories may benefit from a phenomenon known as the "Pygmalion effect," whereby teachers will have higher expectations of those students leading to an increase in performance. Students with poor histories may suffer from the "Golem effect," whereby teachers will have lower expectations placed upon them leading to poorer performance.[4]

Q: What should I do if I believe my child's rights have been violated?

A: If you believe that your rights under any federal law have been violated, including FERPA, PPRA, or COPPA, you should notify your school, district Superintendent, and/or school board as soon as possible. If they refuse to take appropriate action, you may contact your local chapter of the American Civil Liberties Union (ACLU) to request help, or file a complaint. For details on how to do so, see Section II.

Need help? Contact the Parent Coalition for Student Privacy at info@studentprivacymatters.org so we can connect you with other supportive groups and/or resources!

Disclaimer: While the goal of the Parent Coalition for Student Privacy and the Campaign for a Commercial-Free Childhood is to provide valuable resources to help you protect student privacy, our suggestions should not be used in place of legal advice from an attorney. For questions on how federal, state, and local laws and policies may apply to your situation, you may wish to seek the advice of a licensed attorney by contacting your local bar association's referral service.

Questions? Visit www.studentprivacymatters.org/toolkit for more information, including free webinars on how to use the resources in this toolkit.

REFERENCES

1. https://nces.ed.gov/programs/slds/stateinfo.asp

2. https://www.hhs.gov/hipaa/for-professionals/faq/513/does-hipaa-apply-to-an-elementary-school/index.html

3. https://fpf.org/wp-content/uploads/2016/11/SOPIPA-Guide_Nov-4-2016.pdf

4. http://www.oxfordbibliographies.com/view/document/obo-9780199846740/obo-9780199846740-0014.xml

APPENDIX A.

Request to inspect education records held by the school, district, or state

I understand the Federal Education Rights and Privacy Act (FERPA), a federal law, gives parents the right to inspect the information in their child's education records, as collected and maintained by the state, district or school. According to the U.S. Department of Education, education records "include but are not limited to grades, transcripts, class lists, student course schedules, health records (at the K-12 level), student financial information (at the postsecondary level), and student discipline files. The information may be recorded in any way, including, but not limited to, handwriting, print, computer media, videotape, audiotape, film, microfilm, microfiche, and e-mail." **Source:** 34 CFR § 99.3 "Education Records" and "Record"

I further understand that the school or district may not charge a fee to search for or to retrieve education records but they may apply a reasonable fee to provide copies of education records, and must provide them in a readable form within 45 days of the request.

As such, please accept this request for access to all personally identifiable information in my child's education records, including the records you are required to maintain regarding disclosures of or requests for my child's personal information from organizations conducting studies for or on behalf of the school, and from Federal, State, or local educational authorities. The records must also include all unauthorized disclosures of my child's information, including instances of data breaches or security hacks. **Source:** 34 CFR § 99.32 Recordkeeping Requirements.

If you estimate that the fees for copies of these records will exceed [*$*_____], please inform me first.

PARENT OR GUARDIAN NAME: _____

STUDENT NAME: _____

STUDENT GRADE: _____ STUDENT ID NUMBER: _____

SCHOOL NAME: _____

DATE: _____

PARENT/GUARDIAN SIGNATURE (IF STUDENT IS UNDER 18): _____

PARENT OR GUARDIAN EMAIL ADDRESS: _____

PARENT'S HOME ADDRESS: _____

PARENT OR GUARDIAN PHONE: _____

STUDENT SIGNATURE (IF STUDENT IS OVER 18): _____

APPENDIX B.

Sample letter to opt out of disclosure of directory information

I understand that the Family Educational Rights and Privacy Act (FERPA), a federal law, allows my school or school district to disclose designated "directory information" to third parties without my written consent, unless I inform the school/district otherwise, and according to any existing policies and/or procedures.

I am submitting this form because: [choose one option]

☐ My child's school or school district does not have a "directory information" policy.

☐ My child's school or school district's existing "directory information" policy does not sufficiently protect my child's privacy.

PARENT OR GUARDIAN NAME: _____

STUDENT NAME: _____

STUDENT GRADE: _____

STUDENT ID NUMBER: _____

SCHOOL NAME: _____

DATE: _____

PARENT/GUARDIAN SIGNATURE (IF STUDENT IS UNDER 18): _____

PARENT OR GUARDIAN EMAIL ADDRESS: _____

STUDENT SIGNATURE (IF STUDENT IS OVER 18): _____

Directory information that I ALLOW the school or district share:

(Note: Check only the information you ALLOW your school or district to share.)

☐ Student name

☐ Telephone numbers (e.g., home, cell, etc.)

☐ Parent personal information (e.g., name, address, phone, email address, etc.)

☐ Photograph

☐ Video or electronic images

☐ Date of birth

☐ Place of birth

☐ Home or permanent address

☐ E-mail address

☐ Dates of attendance

☐ Weight/Height

☐ Enrollment Status

☐ Grade

☐ Most recent school or educational institution attended

☐ Participation in officially recognized activities and sports

☐ Degree(s) received

☐ Awards and honors received

☐ Clubs/Affiliations

☐ School or district issued student ID number*

***NOTE:** A student ID number may or may not be considered as directory information depending on how the school/district uses it. For more information, see the U.S. Department of Education's Frequently Asked Questions website at www.familypolicy.ed.gov/faq-page [1]

I ALLOW those elements of my child's directory information checked above to be shared only with the following parties:

☐ In school or district publications, including a yearbook, graduation program, theater playbill, athletic team or band roster, newsletter, and other such publications.

☐ With the U.S. Military.

☐ With colleges and other educational institutions.

☐ With prospective employers.

☐ With political officers.

☐ With the National Student Clearinghouse.

☐ With news media.

☐ With the school PTA or district parent organization.

☐ With other groups and entities outside of the school or district, including community, advocacy and/or parent organizations.

☐ With companies that are selling products or services.

☐ With charter schools or mailing houses used by charter schools to send recruiting materials to families.

☐ On official school-related websites or social media accounts.

☐ On school employees' personal websites or social media accounts.

☐ To sign up my child for online educational tools or classroom applications (apps).*

***NOTE:** FERPA allows a school or school district to share a wider array of students' personal information — beyond directory information — with individuals or companies offering operational services, online educational tools or classroom applications (apps) without parental knowledge or consent, or allowing for opt out, as well as for research or evaluation purposes.[2]

REFERENCES

1. U. S. Department of Education, Family Educational Rights and Privacy Act (FERPA) Model Notice for Directory Information.
See http://familypolicy.ed.gov/content/ferpa-model-notice-directory-information

2. U.S. Department of Education, Privacy Technical Assistance Center, FERPA Exceptions - Summary.
See http://ptac.ed.gov/sites/default/files/FERPA%20Exceptions_HANDOUT_horizontal_0.pdf

APPENDIX C.

Sample letter to opt out of military recruitment

NOTE: This form is for use by parents of high school students.

I understand that Section 8025 of the Every Student Succeeds Act (ESSA), a federal law, permits me to submit a written request to the school and/or school district prohibiting the disclosure of my child's information, including my child's name, address, and telephone number, to any United States military recruiter without my prior written consent.[1,2] Please be informed that this document constitutes my written request to bar disclosure.

PARENT OR GUARDIAN NAME: _____

STUDENT NAME: _____

STUDENT GRADE: _____

STUDENT ID NUMBER: _____

SCHOOL NAME: _____

DATE: _____

PARENT/GUARDIAN SIGNATURE (IF STUDENT IS UNDER 18): _____

PARENT OR GUARDIAN EMAIL ADDRESS: _____

STUDENT SIGNATURE (IF STUDENT IS OVER 18): _____

REFERENCES

1. See [[Page 129 STAT. 2115]] https://www.congress.gov/bill/114th-congress/senate-bill/1177/text#toc-H7549C9B976024930B024320484A07993

2. Section 8025 of the Every Student Succeeds Act (ESSA), requires schools and/or school districts to notify parents of secondary school students of their option to refuse the release of their student's name, address, and telephone number to any United States military recruiter that requests it.

APPENDIX D.
Additional questions to ask your teacher or principal

Check out Section V for a list of introductory questions you can ask your child's teacher. Here are additional questions you can ask.

Questions to ask about student information the school or district collects, uses and shares

WHAT KIND OF INFORMATION DOES THE SCHOOL OR DISTRICT COLLECT about students and why? Who is it shared with? Will parents be notified about which personal data is collected or shared, as is considered best practice?[1]

HELPFUL HINT:

The U.S. Department of Education Privacy Technical Assistance Center recommends that schools and/or districts should:

- Develop and publish a data inventory listing the specific information it collects from or about students; and
- Explain why it collects each piece of student information (e.g., for state or federal reporting, to provide educational services, to improve instruction, to administer cafeteria services, etc.).

IF DATA IS STORED IN A STUDENT INFORMATION SYSTEM (SIS), like InfiniteCampus or PowerSchool, who has access to my child's data, and what are they permitted to do with it? Can only her/his teachers, counselor and principal see it, or can other teachers and district officials access it? What about individuals or organizations outside the school or district?

IF I WOULD LIKE TO ACCESS AND REVIEW my child's information stored in his or her education records as well as the data in the SIS, as is my right under federal law, how can I do this?

WILL THE SCHOOL INFORM PARENTS when there is a breach of their children's data by the school or district? What methods will be used to inform parents, and how quickly will it happen?

WHEN WILL THE SCHOOL OR DISTRICT DELETE my child's personal data? Once she/he graduates from high school, or if we move? And will all data be deleted or just some of it?

Questions to ask about student information the district shares with the state department of education, the federal government or researchers

EXACTLY WHAT STUDENT INFORMATION is the school or district required to share with the state education department?

IF I WOULD LIKE TO ACCESS AND REVIEW this information for my child, as is my right under federal law, how can I do this?

IF THE SCHOOL OR DISTRICT PARTICIPATES IN A STUDY by independent researchers or the U.S. Department of Education, will they notify parents before sharing personal student information and explain why de-identified or aggregated data are not sufficient for the study?

IF YOU DON'T KNOW the answers to the above questions, who should I ask?

Questions to ask about your child's use of online programs and classroom applications (apps)

- WHICH CLASSROOM APPS and online programs are going to be assigned to my child, and what are their privacy policies?

HELPFUL HINT:

The U.S. Department of Education Privacy Technical Assistance Center recommends that schools and/or districts "provide parents with a list of online educational services or 'apps' that are approved for use in the classroom."

- DO YOU KNOW WHAT INFORMATION VENDORS COLLECT about my child, how it is being used, and with which other third parties or contractors the vendors may be sharing the data?
- IS THE VENDOR OR CONTRACTOR ALLOWED to use my child's data for marketing purposes? Will my child see ads as part of the program, or will ads be delivered to my child or to me? If so, how can we opt out of this?

HELPFUL HINT:

If your child is under the age of 13, the federal law known as COPPA requires your school to know how the company will use your child's private information before they are allowed to sign up your child to use the classroom app or online program on your behalf. If the company will use your child's private information for any purpose outside of the educational context, the school (or a teacher) may not sign up your child for that classroom app or online program without your permission.

- HAVE THESE PROGRAMS BEEN VETTED by the school, districts, or state for privacy and security? If so, what are the standards for approval?
- IF NOT, WHAT ACTIONS HAVE YOU TAKEN TO ENSURE that my child's data will be safe from breach or abuse, and to ensure that these apps comply with state or federal law?
- HOW CAN I ACCESS AND REVIEW my child's private information held by these companies and/or request that the information be deleted?

HELPFUL HINT:

Schools or districts that designate companies as "school officials," and then disclose students' personally identifiable information from education records to them, should consider their obligations under the federal law known as FERPA. According to the U.S. Department of Education Privacy Technical Assistance Center: "Whenever a provider maintains a student's education records, the school and district must be able to provide the requesting parent (or eligible student) with access to those records. Schools and districts should ensure that their agreements with providers include provisions to allow for direct or indirect parental access."

- IF I REFUSE TO ALLOW MY CHILD TO USE one or more of the classroom apps or online programs, what alternative forms of instruction and assessment will be made available to my child?
- WILL THE SCHOOL INFORM PARENTS when there is a breach of student data by a third party or service provider? If we learn of such a breach, what will be done to minimize impacts? Does the vendor have any liability or responsibility to provide credit monitoring or a credit freeze for families who are affected?

HELPFUL HINT:

Also known as a security freeze, a credit freeze lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. If you believe you or your children are a victim of identity theft, visit https://www.identitytheft.gov/

Questions to ask about one-to-one computing (1:1) and bring your own device (BYOD) programs

- WHEN USING A SCHOOL-ISSUED DEVICE, does the school/district or the company that provided the device have access to my child's emails, video chats, pictures, documents, or other content? Will my child's information be monitored, collected, or recorded?
- CAN MY CHILD USE HER/HIS OWN DEVICE? If so, what information will be monitored or collected by the school?
- IF THERE ARE DEFAULT SETTINGS on school-provided devices to collect personal student data, how can the school or I change those defaults?

HELPFUL HINT:

Schools and districts often use Chromebooks, pre-loaded with Google's G Suite for Education (G Suite), for their 1:1 programs. The Electronic Frontier Foundation recommends changing the Chromebook and G Suite default settings to improve student privacy. Step-by-step instructions can be found at https://www.eff.org/issues/student-privacy/device-settings

- WILL MY CHILD'S DATA collected from school-issued devices be de-identified?
- WILL THE SCHOOL/DISTRICT or party that provided the school-issued device have remote access to the device? If so, who can access my child's device—the school system administrator, people who work for the software company, administrators, teachers, or more?
- CAN EITHER THE PROVIDER or the school turn on the web cam or audio device of a school-issued device? Are they able to remotely access files and documents or view the device screen?

HELPFUL HINT:

A Pennsylvania school district admitted that it remotely accessed the webcams of school-issued laptops, secretly taking pictures of students in their own homes. The spying incident prompted the district to pay $61,000 to settle multiple lawsuits.[2]

- DOES THE SCHOOL have physical or remote access to my child's passwords on the device?
- IF I DON'T WANT my child to be monitored and tracked, will my wishes be respected? Can my child still participate in the one-to-one or BYOD program?
- DOES THE SCHOOL use location tracking software to monitor the location of school-issued devices? If so, who can access the location of my child's device and under what circumstances?
- DO SPECIAL RULES APPLY if other members of our family use the school-issued device?
- WHO IS RESPONSIBLE if the school-issued device breaks or is lost?

Questions to ask about online learning in general

These questions have been adapted from materials developed by Parents Across America. To learn more, visit www.parentsacrossamerica.org

- HOW MUCH TIME PER DAY in school is my child spending on an electronic device?
- HOW MUCH ADDITIONAL TIME, if any, is my child being asked to spend on an electronic device outside of school hours?
- HOW MUCH IS THIS PROGRAM COSTING the school or district?
- IS THE VENDOR PLANNING TO PROFIT by using my child's data for marketing or other commercial purposes?
- FOR EACH SPECIFIC PROGRAM attached to an electronic device that my child is using, please share the purpose of the program, the reason for its inclusion in the curriculum, and evidence of its effectiveness.

If you don't receive sufficient answers to your questions, consider advocating against excessive use of online programs with strategies outlined in Section VI, or consider having your child opt out of one or more of these programs.

Questions? Visit www.studentprivacymatters.org/toolkit for more information, including free webinars on how to use the resources in this toolkit.

REFERENCES

1. http://ptac.ed.gov/sites/default/files/LEA%20Transparency%20Best%20Practices%20final.pdf

2. http://www.cbsnews.com/news/610k-settlement-in-school-webcam-spy-case/

APPENDIX E.
Sample petition

Petitions are a powerful tool to support your advocacy efforts. Ask parents to sign paper or online petitions to get the attention of the school community, press, and decision-makers. Keep the email addresses of those who signed to update them and involve them in ongoing advocacy efforts. Be sure to hold on to the original version and send copies to decision makers.

Sample petition

To: Superintendent of Smithville Unified Schools Paul Harris
CC: Smithville Unified School Board
Mayor of Smithville Reginald Hayes

We Demand Better Privacy Protections for SUSD Students

In the wake of a breach of educational software called Edufile, we demand that Smithville Unified School District (SUSD) cease using this program and take immediate steps to protect sensitive student data. We have learned that SUSD's privacy and security policies are outdated, do not properly defend against breaches and do not bar vendors against using personal student data for advertising, marketing or other commercial purposes.

Technology can play an important role in education but it shouldn't come at the expense of our children's privacy or safety, or be used for advertising which is distracting and undermines their ability to learn. We urge the district to adopt policies that incorporate the Five Principles for Student Privacy as articulated by the Parent Coalition for Student Privacy:

TRANSPARENCY: Parents must be notified in advance of any disclosure of personal student information to any individuals, companies or organizations outside of the school or district, and the contracts posted or available on demand.

NO COMMERCIAL USES: Personal student data should not be used for advertising, marketing, or other business purposes.

SECURITY PROTECTIONS: At minimum, this should include encryption, security training for all individuals with access to the data, and security audits by an independent recognized auditor.

PARENTAL/ STUDENT RIGHTS: No re-disclosures to additional third parties, whether individuals, sub-contractors, or organizations, should be allowed without parental notification and consent.

STRONG ENFORCEMENT MECHANISMS: Fines should be required and parents allowed to sue if the vendor violates the terms of the contract or the law.

Name	School/Organization	Phone	Email

APPENDIX F.
Tips for media outreach and sample press materials

When holding a town hall meeting or other gathering to educate and advocate on issues related to student privacy, don't forget to invite the press by sending a "media advisory." Use our helpful tips and the sample below to begin writing your own today!

How to write a media advisory

STEP 1: Start with today's date.

STEP 2: Select a contact for your group, including the individual's name, phone number, and email address, who will respond to reporters' queries. Other people in your group can and should speak to media, but it's good to have a one person in charge.

STEP 3: Pick a concise and catchy title.

STEP 4: Write a brief description of your event.

STEP 5: Add the "Five Ws" (see sample below).

STEP 6: Conclude with a reminder for interested media to connect with your contact, and provide details.

STEP 7: Place three hashtags or number signs (###) at the end of your advisory.

STEP 8: Send your advisory to local newspapers, television and radio stations one week before your event.

STEP 9: Follow up with phone calls to make sure your advisory was received and to ask if they will be sending someone to cover your event.

STEP 10: Send your advisory again the day before the event, no later than 2 pm.

NOTE: You should send the media advisory in the body of an email. Include the date of the event in the subject line, telling what, where, and when.

Sample media advisory

Date: October 20, 2017 Contact: Lynn Jones, (555 -555-1212; lynn.jones1982@gmail.com)

Smithville Parents To Host Student Privacy Forum

Increasingly, the Smithville Unified School District (SUSD) is mandating that students use online programs and apps for in-school assignments and homework. Yet the district has no procedure for vetting the privacy policies of those apps, and one app used by SUSD middle schoolers was breached last year. Smithville parents asked SUSD officials to host a public forum to address privacy concerns, but they refused. So Smithville Parents for Student Privacy will host their own forum to discuss what SUSD can do to better protect sensitive student data.

WHAT: Smithville Student Privacy Forum
WHO: Speakers include parent Jill Brown; SUSD senior John Doe; 4th grade teacher Frank Allen; and privacy expert Dr. Rhonda Little, Professor of Computer Science, Smithville University
WHERE: 100 Main Street, Smithville
WHEN: Tuesday, April 12, 2017 at 7:00 PM.

WHY: Current SUSD policies do not adequately protect sensitive student data.

For more information, or for news organizations interested in covering this event, please contact Lynn Jones at 555-555-1212 or lynn.jones1982@gmail.com

###

While media advisories are teasers to get media to cover an event, press releases tell a whole story and don't necessarily have to be linked to an event. Because local papers will sometimes quote from press releases without any changes, your release should include everything necessary to tell your story. It should also be written to capture the attention of reporters who may want to follow-up and write their own stories.

How to write a press release

STEP 1: Start with today's date.

STEP 2: Select a contact for your group, including the individual's name, phone number, and email address, who will respond to reporters' queries.

STEP 3: Add the statement "For Immediate Release"

STEP 4: Pick a concise and catchy headline.

STEP 5: Keep your release to one and a half pages. If you're hosting an event, briefly describe details of the event, the participants, and the issue discussed. Include quotes and soundbites. If there's a newsworthy event such as a data breach or the publication of new privacy research that you can link your local efforts to, it may make your release more compelling. Include important details about any contact with the school or experts. The point isn't to embarrass school officials or violate their confidence, but to demonstrate to the press that you have already engaged officials about your concerns. Include any recommendations or demands, such as to improve privacy policies or schedule public hearings.

STEP 6: Conclude with a strong quote.

STEP 7: Place three hashtags or number signs (###) at the end of your release.

STEP 8: Send your press release in the body of an email after the event to local newspapers, television and radio stations, and parents, officials, and others who could not attend.

Sample press release

Date: October 20, 2017
Contact: Lynn Jones, (555 -555-1212; lynn.jones1982@gmail.com)
For Immediate Release

Coalition Demands Better Privacy Protections for SUSD Students

SMITHVILLE, NC — In the wake of a recent hack of educational software that left millions of students' personal information vulnerable, a coalition of concerned parents and teachers is demanding that Smithville Unified School District (SUSD) take immediate steps to protect sensitive student data. The coalition says that SUSD's privacy policies are outdated and don't reflect the growing use of apps and cloud based services by the district.

"Technology can play an important role in education but it shouldn't come at the expense of privacy," said Phillip Grant, a Smithville High School parent. "In today's digital era, our student data is a valuable commodity and it's not clear to me that SUSD is taking the necessary precautions to protect against commercial misuse or hacking."

The coalition first reached out to school officials after hackers infiltrated Edufile, a cloud-based system that allows approved district vendors to access student data. On February 18th, a group of concerned parents met with Superintendent Paul Harris. During that discussion, it became apparent that SUSD's privacy policies were deficient and didn't even prohibit the use of apps that collected personal information from students for marketing purposes.

"I was shocked to discover that the online program my daughter was assigned to use for homework was compiling a dossier of her likes and interests," said Jill Brown, a parent of a Smithville Middle School student. "I understand why free apps would be appealing to a teacher, but I don't want my daughter paying for her education with her privacy."

The coalition is urging the district to adopt policies that incorporate the national Parent Coalition for Student Privacy's principles to protect student privacy, available at http://www.studentprivacymatters.org/five-principles-to-protect-study-privacy. Those principles include:

- Transparency: Parents must be notified by their children's school or district in advance of any disclosure of personal student information to any persons, companies or organizations outside of the school or district. All disclosures to third parties should also require publicly available contracts and privacy policies that specify what types of data are to be disclosed for what purposes, and provide a date certain when the data will be destroyed.

- No commercial uses: Selling of personal student data and/or use for marketing purposes should be banned. NO advertising should be allowed on instructional software or websites assigned to students by their schools, since ads are a distraction from learning and serve no legitimate educational purpose.

- Security protections: At minimum, there must be encryption of personal data at motion and at rest, required training for all individuals with access to personal student data, audit logs, and security audits by an independent auditor. Passwords should be protected in the same manner as all other personal student information.

- Parental/student rights: NO re-disclosures by vendors or any other third parties to additional individuals, sub-contractors, or organizations should be allowed without parental notification and consent (or students, if they are 18 or older).

Added Grant, "As a parent, I should have the right to control who has access to my child's personal information."

# # #

ADDITIONAL RESOURCES

Resources on Federal Laws Protecting Student Privacy

FAMILY EDUCATION RIGHTS AND PRIVACY ACT (FERPA): see U.S. Department of Education's Family Policy Compliance Office website at familypolicy.ed.gov/ferpa-parents-students

PROTECTION OF PUPIL RIGHTS AMENDMENT (PPRA): see U.S. Department of Education's Family Policy Compliance Office website at familypolicy.ed.gov/ppra

INDIVIDUALS WITH DISABILITIES ACT (IDEA): see U.S. Department of Education's Office of Special Education and Rehabilitative Services website at www2.ed.gov/about/offices/list/osers/osep/osep-idea.html

NATIONAL SCHOOL LUNCH ACT (NSLA): see U.S. Department of Agriculture's Food and Nutrition Service website at www.fns.usda.gov/nslp/history_5

CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA): see Federal Trade Commission's website at www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Resources for Parents and Advocates

For general guidance and resources, the U.S. DEPARTMENT OF EDUCATION'S PRIVACY TECHNICAL ASSISTANCE CENTER website at ptac.ed.gov

For more information about the ELECTRONIC PRIVACY INFORMATION CENTER'S (EPIC) Student Privacy Project, visit epic.org/privacy/student

To learn about the ELECTRONIC FRONTIER FOUNDATION'S (EFF) Spying on Students: School-Issued Devices and Student Privacy initiative and accompanying report, see www.eff.org/issues/student-privacy

To access PARENTS ACROSS AMERICA'S resources about "personalized learning" and limiting children's screen time, visit parentsacrossamerica.org

THE AMERICAN CIVIL LIBERTIES UNION (ACLU) advocates for stronger privacy rights for students and others; see www.aclu.org/map/takectrl-nationwide-privacy-push

Resources to Share with Schools and School Districts

FORDHAM LAW SCHOOL'S CENTER ON LAW AND INFORMATION POLICY offers a classroom curriculum on student privacy at www.fordham.edu/info/24071/privacy_education

THE CONSORTIUM FOR SCHOOL NETWORKING (COSN), a professional association for school technology leaders, offers a student data privacy and security toolkit at cosn.org/sites/default/files/CoSN-Privacy-Toolkit.pdf

THE STUDENT DATA PRIVACY CONSORTIUM (SDPC) is a collaborative of schools, districts, regional and state agencies addressing solutions to student data privacy concerns. More information here: https://secure2.cpsd.us/a4l

For privacy evaluations of specific educational software and programs, visit COMMON SENSE MEDIA at www.commonsense.org/education/privacy

And don't forget our websites, Campaign for a Commercial-Free Childhood at www.commercialfreechildhood.org
Parent Coalition for Student Privacy at www.studentprivacymatters.org