FPF Student Privacy
Train-the-Trainer Program
Module 1: Protecting Student Privacy
CLE Materials

March 27, 2020

Module 1: Protecting Student Privacy

March 27, 2020

TABLE OF CONTENTS

Note: FPF is happy to provide any or all CLE materials upon request.

Module 1 Activities

There are two individual activities for this module.

1. The Federal Student Privacy Laws Overview Chart
2. The PPRA Exercise

Please complete the activities in this document and email the document to ttt@fpf.org by **March 17th**.

Federal Student Privacy Laws
Overview Chart

After reviewing the resources for this module, please complete the following chart. The first row has been completed as an example.

	Regulated Entities	**Purpose**	**Notification Needed?**	**Consent Required?**
FERPA (USDOE) *Example*	*Educational agencies and institutions*	*Ensure parents have control over their child's education records/data*	*Rights; Directory Information*	*Yes, or an approved exception*
PPRA (USDOE)				
COPPA (FTC)				
CIPA (FCC)				

PPRA Exercise

Based on your understanding of PPRA, list which questions on the **College Board's SAT Student Data Questionnaire** require parental consent prior to being asked to minors and identify which sensitive issues are implicated.

Module 1: Protecting Student Privacy

March 27, 2020

FERPA Exceptions

1. School Official
    a. A school official is someone that has a legitimate educational interest in a student
    b. School officials must be performing a function the school would otherwise perform themselves; must only use the data for the reason it was given to them; and must be under the school's direct control in regards to the use and maintenance of the data
2. Directory Information
    a. Directory information is information generally considered not to be harmful or an invasion of privacy if released to the public
    b. Examples include a student's name, gender, birthdate, picture, grade level, SSID, height, etc.
    c. Each LEA or school designates what they think is directory information
    d. Parents must be given an annual notification of what types of data are designated as directory information
    e. Parents must be given the option to opt out of directory information
    f. Parents must be given a time frame in which they can opt out
3. Audit and Evaluation
    a. Entity receiving the data has to be a state or local educational authority, or an authorized representative of such an authority
    b. A written agreement must be in place that ensures the data are only used for the authorized purpose
    c. Data must be destroyed when it is no longer needed for the audit or evaluation
4. Studies
    a. Under the studies exception, schools can share student PII to develop, validate, or administer predictive tests; administer student aid programs; and improve instruction

    b. Data can only be shared with a written agreement that details the purpose, scope, and duration of the study; what data are to be shared; and that data can only be used for the purposes of the study
5. Health and Safety Emergency
    a. Schools may disclose student PII in an emergency if it will help protect the health or safety of the student or other individuals
    b. Schools should take into account the totality of the threat based on information available at the time
    c. Schools should only share information if there is an articulable and significant threat to the student or others
    d. Schools should only share information with individuals whose knowledge of the situation is necessary to protect the health or safety of the student
    e. Disclosures between other state agencies should not be routine or normal and only shared if there is an imminent emergency
6. Student Transfer
    a. Schools can share student information with each other without parental consent when a student is transferring
    b. Schools need to make a reasonable attempt to notify parents of the exchange
    c. Including that your school will forward records in the case of student transfer in your annual FERPA notice will help simplify the process
    d. Any previously attended school may share records with the new school
7. Parents and Students
    a. LEAs may disclose student data to the parents of the student and to the students themselves
8. Dependent
    a. If a parent claims a student as a dependent on their taxes as defined in Section 152 of the Internal Revenue code of 1986, the school may share student data with parents if the student has already turned 18
9. Sex Offenders
    a. If the disclosure relates to sex offenders or other individuals required to register under Section 170101 if the Violent Crimes Control and Law Enforcement Act of 1994
10. Accrediting Purposes
    a. You may disclose student PII to an accrediting organization so they can carry out their accrediting functions
11. Financial Aid

a. LEAs may disclose student records in connection with financial aid the student has applied for or received
b. Records should help determine the amount; eligibility; and conditions of the aid, or to enforce the terms and conditions of the financial aid

12. Juvenile Justice
    a. LEAs may disclose student records with state and local authorities of the juvenile justice service so long as a state statute allows it
    b. If the state statute was passed after 1974, the disclosure has to relate to the system's ability to effectively serve the student prior to adjudication
    c. If the statute was passed before 1974, different restrictions apply
13. Child Nutrition
    a. You can share student education records with:
        i. USDA, their authorized representative, or a contractor working for Food and Nutrition Services for the purposes of program monitoring; evaluations; or performance measurements of state or local agencies
    b. Only for schools receiving funds under the Richard B Russell School Lunch Act or the Child Nutrition Act
    c. Only the authorized representative should have access to the PII
    d. You may share the results as aggregate data
    e. Data should be destroyed once it is no longer needed
    f. Child nutrition data is also protected by the National School Lunch Act and PPRA
14. Case Workers
    a. Schools may share records with caseworkers or other representatives of state or local child welfare agencies or other tribal organizations.
    b. Records may only be shared with caseworkers if:
        i. They have the right to access the student's case plan
        ii. The student is under the "care and protection" of the agency
            1. Consult your local law when defining "case and protection"
    c. The caseworker may not redisclose the records to unauthorized individuals
15. Judicial Order
    a. LEAs must share data in order to comply with a judicial order or a legally issued subpoena, but they shouldn't immediately share records.
        i. Consult with your legal counsel.
        ii. LEAs should notify parents or eligible students of the subpoena within a reasonable amount of time so they may seek protective action unless
            1. it is a federal grand jury subpoena;
            2. the subpoena specifically orders the content not be disclosed; or

3. it is an ex parte court order in relation to a terrorism investigation

iii. The school can also seek protective action when they believe the student's privacy needs outweigh the defendants' need to access the data

16. Disciplinary Proceeding: alcohol or a controlled substance
    a. This exception only applies to postsecondary schools
    b. If the disciplinary proceeding is in regards to the use or possession of alcohol or a controlled substance, you may share the violation with the parents if:
        i. The student did commit the violation
        ii. The student is under 21 at the time of the disclosure
    c. This provision does not supersede any state law that would otherwise prohibit the disclosure.
17. Disciplinary Proceeding: violence or non-forcible sex offense
    a. This exception only applies to postsecondary schools
    b. Two things determine what results you can share:
        i. The type of offense committed
        ii. Whom you're sharing the results with
    c. If they committed a crime of violence or a non-forcible sex offense (FERPA has a list)
        i. You may share final results with:
            1. Victim, regardless of whether they determined a violation was committed or not
            2. Others, only if they determined a violation was indeed committed
        ii. You can only share this information about the final result:
            1. The name of the student who committed the violation
            2. The violation committed
            3. Any sanctions against the student
        iii. You may not disclose the names of any other students, including victims or witnesses, without prior consent
        iv. Only applies to results reached after October 7, 1998

FUTURE OF PRIVACY FORUM

TRAIN THE TRAINER

MODULE 1 WEBINAR

MODULE 1 OBJECTIVES

1. Demonstrate an understanding of the federal student privacy laws
2. Compare and contrast the various federal student privacy laws
3. Communicate how these laws impact the day-to-day work of educational institutions

MODULE 1 ACTIVITIES

	Target Audience	Purpose	Notification	Consent
FERPA (USDOE)	Educational institutions	Ensure parents have control over their child's education records/data	Rights Directory information	Yes, or an approved exception
PPRA (USDOE)	Educational institutions	Protect the privacy of students in the administration of surveys, medical exams, and marketing	Rights Specific applicable events Policies	Yes, by parent
COPPA (FTC)	Online providers	Ensure that children under 13 do not enter personal information on the internet without consent of parents	Post privacy policy Rights PII collected and use	Yes, by parent or school acting on behalf of parent
CIPA (FCC)	Educational institutions and libraries receiving E-Rate funding	Protect children from obscene online content	How students are being monitored must be included in the schools' internet safety policies. Notice and public hearing	N/A

PPRA EXERCISE

If your school is using the SAT as a Title I assessment, or are pre-populating any information on the pre-test survey (like a student grade or ID number), schools must obtain parental consent before students take these surveys. These surveys often directly ask students about PPRA-protected topics like their **parents' income (#34)**, **religion (#31)**, or **citizenship (#30)** in order to provide that information to higher education institutions, scholarship organizations, and education non-profits. Even if the surveys do not ask about PPRA-protected topics, your school may still need to get parental consent for students to take these surveys under FERPA depending on whom the data are being shared with.

Additional Resources

PTAC, Technical Assistance on Student Privacy for State and Local Educational Agencies When Administering College Admissions Examinations

FPF, Dept of Ed: Parents, Not Minor Students, Must Consent to College Admissions Pre-Test Surveys and Data Sharing

PRESENTATION

Amelia Vance
Director
Youth and Education Privacy
Future of Privacy Forum

FUTURE OF PRIVACY FORUM

TRAIN THE TRAINER

A Taxonomy of Privacy (compiled from Solove 2006)

Domain	Privacy breach	Description
Information Collection	*Surveillance*	Watching, listening to, or recording of an individual's activities
	Interrogation	Various forms of questioning or probing for information
Information Processing	*Aggregation*	The combination of various pieces of data about a person
	Identification	Linking information to particular individuals
	Insecurity	Carelessness in protecting stored information from leaks and improper access
	Secondary Use	Use of information collected for one purpose for a different purpose without the data subject's consent
	Exclusion	Failure to allow the data subject to know about the data that others have about her and participate in its handling and use, including being barred from being able to access and correct errors
Information Dissemination	*Breach of Confidentiality*	Breaking a promise to keep a person's information confidential
	Disclosure	Revelation of information about a person that impacts the way others judge her character
	Exposure	Revealing another's nudity, grief, or bodily functions
	Increased Accessibility	Amplifying the accessibility of information
	Blackmail	Threat to disclose personal information
	Appropriation	The use of the data subject's identity to serve the aims and interests of another
	Distortion	Dissemination of false or misleading information about individuals
Invasion	*Intrusion*	Invasive acts that disturb one's tranquillity or solitude
	Decisional Interference	Incursion into the data subject's decisions regarding her private affairs

FUTURE OF PRIVACY FORUM
TRAIN THE TRAINER

Kitchin, Rob. (2016). Getting smarter about smart cities: Improving data privacy and data security. https://www.researchgate.net/publication/293755608_Getting_smarter_about_smart_cities_Improving_data_privacy_and_data_security; https://www.slideshare.net/robkitchin/privacy-maynooth

“Computerized record-keeping systems by several school districts may make detection errors somewhat more difficult unless extreme care is taken by school personnel…the more frequently that records are examined…the more likely it is that mistakes will be discovered and corrected. The eventual widespread use of computers in schools, therefore, should be accompanied by policies encouraging more frequent access to school records by parents, as well as school personnel.”

Table 5. Number of School Districts Reporting that Various Individuals Have Access to Entire Permanent Record, to Part of the Record, or to None of It.

Individuals	Have access to entire file	Denied access to entire file	Denied access to part of file	Access depends on circumstances	No answer[a]	Total
School nurse	31	0	10	4	7	51[b]
Teachers	43	0	3	3	5	54
Parents, guardians, etc.	8	20	14	8	4	54
Prospective employers	9	20	16	5	4	54
Pupils	5	26	13	7	3	54
Juvenile courts (without subpoena)	23	12	7	6	6	54
Local police officials	18	14	9	8	5	54
Health Department officials	21	18	5	5	5	54
CIA, FBI officials	29	12	1	8	4	54

[a]Includes inappropriate responses or conflicting answers.
[b]Three school systems reported "no nurse."

"One program instructed kindergarten teachers in sophisticated methods of identifying 'target students'—those five-year-olds whose social and academic profiles were similar to those of adolescents who ended up in juvenile courts...suddenly, an unwary kindergarten teacher has become in effect a government intelligence agent."

Diane Divoky, National Committee for Citizens in Education, 1974

"One of the more serious abuses has been the insertion of potentially prejudicial anecdotal comments and factual inaccuracies into the children's school records. When parents and students are not allowed to inspect school records and make corrections, such material can have devastatingly negative effects on the academic future and job prospects of an innocent, unaware student."

Senator Buckley, May 1974

"As the process of information collection in the schools snowballed—a few more forms for the guidance department, a few more facts for state agencies, another set of teacher comments for a new tracking plan—almost no one stopped to weigh the implications of recording; so much hard and soft data about children and their families. There was little thought given to development of clean policies and practices by which student and parental rights of privacy might be balanced against the needs of the school and other social agencies to know, or to guarantee, that material contained in records was accurate and pertinent."

Cong. Rec. S. Nov. 19, 1974 p. 36529

DEPT OF HEALTH, EDUCATION, AND WELFARE 1973 FIPS

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for a person to find out what information about the person is in a record and how it is used.
- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
- There must be a way for a person to correct or amend a record of identifiable information about the person.
- Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Fair Information Practice Principles	
Principle	**Description**
Notice	Individuals are informed that data are being generated and the purpose to which the data will be put
Choice	Individuals have the choice to opt-in or opt-out as to whether and how their data will be used or disclosed
Consent	Data are only generated and disclosed with the consent of individuals
Security	Data are protected from loss, misuse, unauthorized access, disclosure, alteration and destruction
Integrity	Data are reliable, accurate, complete and current
Access	Individuals can access, check and verify data about themselves
Accountability	The data holder is accountable for ensuring the above principles and has mechanisms in place to assure compliance

https://www.slideshare.net/robkitchin/privacy-maynooth

FUTURE OF PRIVACY FORUM

TRAIN THE TRAINER

FERPA

FUTURE OF PRIVACY FORUM

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

- Gives parents (and eligible students) the right to access and seek to amend their children's education records
- Protects **personally identifiable information** (PII) from **education records** from unauthorized disclosure
- Requires **written consent** before sharing PII – **unless an exception applies**

(20 U.S.C. §1232g & 34 CFR Part 99)

TO WHICH EDUCATIONAL AGENCIES AND INSTITUTIONS DOES FERPA APPLY?

Elementary

Secondary

Postsecondary

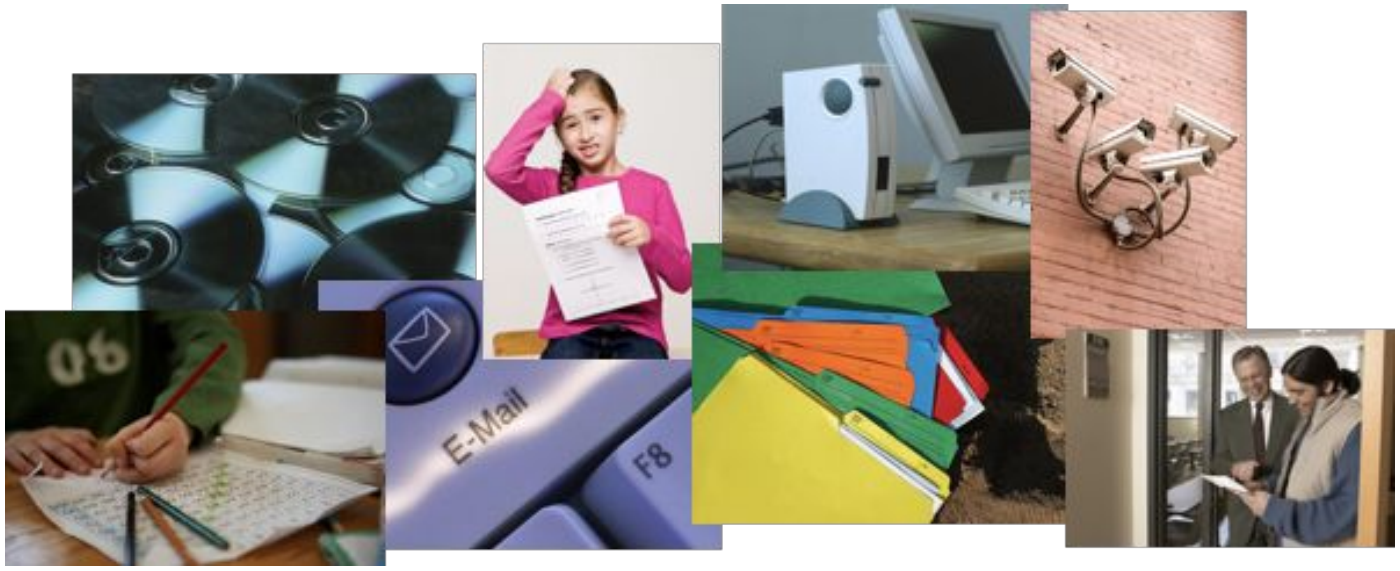
+

U S D E P T O F E D

JUST WHAT IS AN EDUCATION RECORD?

"Education records" are records 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.



PERSONALLY IDENTIFIABLE INFORMATION (PII)

- **Direct Identifiers**
  - e.g., Name, SSN, Student ID Number, etc.

  (1:1 relationship to student)

- **Indirect Identifiers**
  - e.g., Birthdate, Demographic Information

  (1:Many relationship to student)

- *"**Other information** that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty." (§ 99.3)*

MAIN PROVISIONS

Grants parents and eligible students the following rights:

- Right to annual notification of school's FERPA policy
- Right of access to child's education records
- Right to seek amendment/correction of child's education records

MAIN PROVISIONS

Grants parents and eligible students the following rights:

- Right to confidentiality of PII in own education records
- Right to file a complaint with Dept of Ed for alleged violations

TWO MAIN GOALS OF FERPA

- **ACCESS**: Guarantees students access to their own educational records; and

- **PRIVACY**: Prevents unauthorized disclosure of educational records

  (unless exception applies…)

ACCESS

- Students have right to inspect and review their own education records
- School must respond to request for inspection within a reasonable time but no later than 45 days
- Prohibits school from deleting or destroying records while access is pending
- Can’t charge unreasonable amount

PRIVACY

- Student's written consent required before disclosure to third parties
- Third party recipients must agree not to re-disclose
- School must keep a record of all third party requests and disclosures
- Allows for non-consensual disclosure in certain limited circumstances

TOP EXCEPTIONS TO CONSENT

- School official exception (§99.31(a)(1))
- Studies and audit and evaluation exceptions (§99.31(a)(6) and §99.31(a)(3))
- Directory information (§99.31(a)(11))
- Health and safety exception (§99.31(a)(10))
- Law enforcement and subpoena (§99.31(a)(3)(ii) and §99.31(a)(9))
- Lawsuit (§99.31(a)(9))

SCHOOL OFFICIAL, STUDIES, & AUDIT AND EVALUATION EXCEPTIONS

We'll talk about these later in the program in detail, so all you need to know is...

The school official exception includes your internal staff and volunteers

DIRECTORY INFORMATION EXCEPTION

- May include:
  - ✓ name, address, phone number, and e-mail address
  - ✓ photograph
  - ✓ date and place of birth
  - ✓ most recent school attended; grade level and major field of study
  - ✓ dates of attendance (e.g., year or semester)
  - ✓ participation in officially recognized sports and activities; height and weight of athletes,
  - ✓ degrees, honors, and awards received, and
- Can never include social security number
- Can't disclose non-directory information with directory information

DIRECTORY INFORMATION EXCEPTION

- Annual notice must be given to parents
- Students may choose to “opt-out” of the disclosure of directory information
- Schools may adopt a limited directory information policy that allows for the disclosure of directory information to specific parties, for specific purposes, or for both.

November 6, 2018

60°

THE ROANOKE TIMES

roanoke.com

Progressive political group obtains cellphone numbers from Virginia Tech, Radford students for electoral campaigns

By Carmen Forman carmen.forman@roanoke.com 981-3334 Oct 3, 2017

POLICY UPDATE

Vol. 25, No. 10
December 2018

National Association of State Boards of Education

Protecting Privacy of School Directory Information

By Amelia Vance

Students do not have the right to attend school anonymously, but they do have a right to have their information protected and used responsibly by local and state education agencies. State boards can help their states strike this balance.

When the Family Educational Rights and Privacy Act (FERPA) was first passed in 1974, schools realized that they had a problem: Without ongoing consent from

shares information with a third party, that third party can redisclose that information to anyone. This is mainly for practical reasons. As mentioned above, schools can use directory information, for example, to create a program for a school play that lists participating students' names. However, as anyone could attend the play and get the program, the school has no way to control who gets this information. If a parent objects, they can opt out of directory information sharing, and the student will not be listed in the program.

To some, sharing contact information may seem innocuous. Yet four districts learned otherwise last fall when malicious hackers attacked their student information systems, used parent and student telephone numbers to text death threats to students, and posted student contact information online.[5] They tweeted, "With the student directory from [Johnston Community School District in Iowa that] we released, any child predator can now easily acquire new targets and even plan based on grade level." While in the past a PTA directory would be photocopied and only shared within a community, today this contact information is often available online instead.

BOX 1. EXAMPLES OF DIRECTORY INFORMATION

HEALTH & SAFETY EXCEPTION

- “The disclosure is in connection with a health or safety emergency, under the conditions described in §99.36…”
- **Necessary to disclose** a student’s education records (or PII contained in those records) to **appropriate parties** in order to **address a specific and articulable threat of a health or safety emergency**.
- **Limited to the period of the emergency** and **does not allow for a blanket release** of PII from a student’s education records.
- Emergency examples: impending natural disaster, a terrorist attack, a campus threat, or the outbreak of an epidemic disease.

HEALTH & SAFETY EXCEPTION: BEST PRACTICES

- Ensure that emergency response plans include clear guidance on when students' personally identifiable information may be disclosed
- Ensure that it is an emergency
- Disclose only the information necessary to resolve specific health or safety situations
- Disclose information only to the appropriate parties - those who need to know
- Carefully consider potential unintended consequences, such as disproportionate effects on vulnerable populations, and balance those risks with the benefits of disclosing student information

HEALTH & SAFETY EXCEPTION RESOURCES

- FPF, Disclosing Student Information During School Emergencies: A Primer for Schools
- FPF, Student Privacy During the COVID-19 Pandemic
- PTAC, FERPA and the Coronavirus Disease 2019 (COVID-19)
- PTAC, School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA)
- The Network for Public Health Law, Data Privacy in School Nursing: Navigating the Complex Landscape of Data Privacy Laws (Part I)
- The Network for Public Health Law, Data Privacy in School Nursing: Navigating the Complex Landscape of Data Privacy Laws (Part II)
- The Network for Public Health Law, Data Sharing Guidance for School Nurses

LAW ENFORCEMENT PURPOSES AND THE SUBPOENA EXCEPTION

- to the “authorized representatives of the Attorney General” (part of the audit and evaluation exception);
- “to comply with a judicial order or lawfully issued subpoena.”
- Records created by a law enforcement unit for a law enforcement purpose and maintained by the law enforcement unit

LAW ENFORCEMENT PURPOSES AND THE SUBPOENA EXCEPTION

- FERPA requires schools to notify the student or parent *before* disclosing records under a subpoena unless a court has ruled otherwise
- SROs are likely acting jointly as a school official and a law enforcement unit, and must segment information collection and sharing accordingly

LAW ENFORCEMENT PURPOSES AND THE SUBPOENA EXCEPTION RESOURCES

- PTAC, School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA)
- FPF, Law Enforcement Access to Student Records: A Guide for School Administrators & Ed Tech Service Providers
- FPF, Disclosing Student Information During School Emergencies: A Primer for Schools

LAWSUIT EXCEPTION

- (iii)(A) If an educational agency or institution initiates legal action against a parent or student, the educational agency or institution may disclose to the court, without a court order or subpoena, the education records of the student that are relevant for the educational agency or institution to proceed with the legal action as plaintiff.
- (B) If a parent or eligible student initiates legal action against an educational agency or institution, the educational agency or institution may disclose to the court, without a court order or subpoena, the student's education records that are relevant for the educational agency or institution to defend itself.

COMMENTARY

Raped on Campus? Don't Trust Your College to Do the Right Thing

By Katie Rose Guest Pryal | MARCH 02, 2015

In January, a rape survivor sued the University of Oregon for mishandling her sexual-assault case. Through the campus judicial process, the university found the three male students responsible for gang-raping her (not the technical term). They were kicked off the varsity basketball team and eventually out of school. But there is a lot more to the story, including the ways that the university delayed the investigation of the students long enough so that they could finish up their basketball season.

The story is long, and it might destroy your faith in humanity, even if the university did drop its counterclaim against the survivor last week. In that counterclaim, Oregon had accused her of "creating a very real risk that survivors will wrongly be discouraged from reporting sexual assaults."

THE CHRONICLE OF HIGHER EDUCATION

The Oregon administration accessed the rape survivor's therapy records from its counseling center and handed them over to its general counsel's office to help them defend against her lawsuit. They were using her own post-rape therapy records against her.

It was a senior staff therapist in the counseling unit who blew the whistle on the administration's actions. In her public letter, she sounds horrified that the work she thought was protected by medical privilege could be violated in such a fashion.

https://www.chronicle.com/article/Raped-on-Campus-Don-t-Trust/228093

The university came firing back, arguing that because the rape survivor had asserted a legal claim of emotional distress, Oregon was entitled under, of all things, the Family Educational Rights and Privacy Act to use her medical records to defend against her suit.

When I read the university's defense of its actions, I had to laugh. Medical privacy typically can be breached in a lawsuit setting only when a patient sues a health-care provider for malpractice. In those instances, the medical records become material evidence to determine whether the provider had breached medical standards of care.

https://www.chronicle.com/article/Raped-on-Campus-Don-t-Trust/228093

THE
LUND REPORT
Oregon's most vital source of health news

Senate Unanimous in Bill Protecting Student Medical Records

SB 1558 closes an end-run that University of Oregon officials made around privacy laws to access a student's counseling records to use against her when she sued the university for its mishandling of her rape case involving the basketball team.

By: Chris Gray

THE
LUND REPORT
Oregon's most vital source of health news

Key Takeaway:

FERPA exceptions are generally *may* share, not *must*. Consider whether it is wise, from a legal perspective, a PR perspective, and, first and foremost, by looking at whether the sharing benefits the student.

OTHER EXCEPTIONS

- To Parents and Students (of course) (§99.31(a)(12))
- Student Transfer (§99.31(a)(2))
- Student as a Dependent (§99.31(a)(8))
- Sex Offenders (§99.31(a)(16))
- Accrediting Purposes (§99.31(a)(7))
- Financial Aid (§99.31(a)(4))
- Juvenile Justice (§99.31(a)(5))
- Child Nutrition
- Case Workers
- Certain Postsecondary Disciplinary Proceedings (§99.31(a)(13-14) and §99.31(a)(15))

REMINDER: Most exceptions are *may* not *must*

ENFORCEMENT

FUTURE OF PRIVACY FORUM

FUTURE OF PRIVACY FORUM

TRAIN THE TRAINER

Education Week reporter Ben Herold explores how technology is shaping teaching and learning and the management of schools. Join the discussion as he analyzes the latest developments.

Benjamin Herold

« Ivanka Trump, Apple's Tim Cook Push STEM, Computer Science Education | Main

Inspector General Blasts U.S. Ed. Department's Handling of FERPA Complaints

By Benjamin Herold on November 29, 2018 4:09 PM

The U.S. Education Department failed to conduct timely, effective investigations of potential violations of the nation's main student-data-privacy law, allowing a years-long backlog of unresolved cases to pile up without any mechanism for effectively tracking the number or status of the complaints it received.

That's according to a **scathing new audit** from the department's own Inspector General, released

FOLLOW THIS BLOG

RECENT ENTRIES

Inspector General Blasts U.S. Ed. Department's Handling of FERPA Complaints

Ivanka Trump, Apple's Tim Cook Push STEM, Computer Science Education

Majority of District Leaders Concerned About Cyber Threats, Project Tomorrow Report Finds

Fortnite, Video Game Popular Among Students, Now Has 200 Million Players

Cybersecurity-Focused High School to Open in Texas in Fall 2019

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF MANAGEMENT

December 20, 2018

Improving the Effectiveness and Efficiency of FERPA Enforcement

The U.S. Department of Education (Department) has determined that this document is significant guidance under the Office of Management and Budget's Final Bulletin for Agency Good Guidance Practices.[1] Significant guidance is non-binding and does not create or impose new legal requirements. The Department is issuing this document to provide educational agencies and institutions with information to assist them on meeting their obligations under section 444 of the General Education Provisions Act, commonly referred to as the Family Educational Rights and Privacy Act (FERPA) and implementing regulations (34 CFR part 99). This document also provides members of the public with information about their rights under the law and regulations. If you are interested in commenting on this document, please email us your comment at Michael.Hawes@ed.gov or write to us at the following address: Michael Hawes, U.S. Department of Education, 400 Maryland Avenue, SW., room 6W113 LBJ, Washington, DC 20202.[2]

The Department is committed to protecting student privacy. To provide more timely and effective assistance to parents and students and to address a recommendation made by the Department's Office of the Inspector General to "implement a risk-based approach to processing and resolving FERPA complaints,"[3] the Department is modifying its investigatory practices to more efficiently address and resolve complaints and violations under FERPA.

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF MANAGEMENT

December 20, 2018

...we have also determined that the best and most reasonable approach to improve processes consistent with law is to ***make a case-by-case determination for every timely complaint to determine the best mechanism for resolving the underlying situation****. Sometimes, the action will be a* ***formal investigation****; for these complaints, we will investigate consistent with the regulatory provisions under Subpart E of part 99. For other complaints, consistent with the statute and applicable regulations, we will take appropriate actions such as* ***acting as an intermediary or providing resolution assistance****.*

The Department is committed to protecting student privacy. To provide more timely and effective assistance to parents and students and to address a recommendation made by the Department's Office of the Inspector General to "implement a risk-based approach to processing and resolving FERPA complaints,"[2] the Department is modifying its investigatory practices to more efficiently address and resolve complaints and violations under FERPA.

FERPA RE-WRITE?

FUTURE OF PRIVACY FORUM

FUTURE OF PRIVACY FORUM

TRAIN THE TRAINER

PPRA

FUTURE OF PRIVACY FORUM

FUTURE OF PRIVACY FORUM

TRAIN THE TRAINER

PROTECTION OF PUPIL RIGHTS AMENDMENT (PPRA)

- Amended in 2001 with No Child Left Behind Act
- Mostly known for its provisions dealing with surveys in K-12
- Includes limitations on using personal information collected from students for marketing
- May require parental notification and opportunity to opt-out
- May require the development of policies in conjunction with parents
- However … a significant exception for “educational products or services”

PPRA

- Political affiliations;
- Mental and psychological problems potentially embarrassing to the student and his/her family;
- Sex behavior and attitudes;
- Illegal, anti-social, self-incriminating and demeaning behavior;
- Critical appraisals of other individuals with whom respondents have close family relationships;
- Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
- Religious practices, affiliations, or beliefs of the student or student's parent*; Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program.)

Note: Inferences aren't included

U.S. Department of Education, PPRA for Parents

PPRA

Student Participation Required	Covers the Eight Protected Categories	Opt-in/Opt-out
Yes	Yes	Provide notice and parents must opt in for the student to take the survey
Yes	No	Provide notice and parents have the right to opt out
No	Yes	Provide notice and parents have the right to opt out (but check your specific state law first)
No	No	Provide notice only if the survey was created by a third party. In that case, parents have the right to opt out.

BE CAREFUL OF SEL/CLIMATE SURVEYS

FUTURE OF PRIVACY FORUM
TRAIN THE TRAINER

“In addition to being denied access to their children's school records, parents are often unable to readily review the instructional materials in various courses in which their children are enrolled. And often they are not asked to give their consent before their child is given very personal or psychological tests, or participate in experimental programs or attitude-affecting courses…

…the most damaging questions in this category are those which extract self-incriminating information from the students themselves on truancy, insolence, and other improper activities in school. Self-confessions by students on such things as fighting in class and telling off the teacher provide an evaluation team with data to be entered into a permanent personality record classifying students as maladaptive, aggressive, antisocial, emotionally disturbed, and predelinquent.”

U.S. DEPARTMENT OF EDUCATION

Protection of Pupil Rights Amendment (PPRA)

FORM APPROVED
OMB NUMBER: 1880-0544
Exp. 07/31/2022

Complaint Form

Instructions: The United States Department of Education's (Department) Student Privacy Policy Office (SPPO) reviews, investigates, and processes complaints of alleged violations of the Protection of Pupil Rights Amendment (PPRA). 20 U.S.C. 1232h and 34 CFR Part 98. PPRA is a federal law that affords certain rights to parents of students attending elementary or secondary schools with regards to any survey, analysis, or evaluation that asks students to reveal information of a personal nature. The rights afforded parents under PPRA transfer to the student when the student turns 18 years old or is an emancipated minor under applicable State law. PPRA also concerns marketing surveys, parental access to instructional material, as well as the administration of certain physical examinations to minors. A local educational agency (LEA), or school district, must provide parents effective notice of their rights under PPRA.

PPRA applies to the programs and activities of recipients of funds under any program funded by the U.S. Department of Education (Department), such as LEA. It governs the administration to students of a survey, analysis, or evaluation that concerns one or more of the following eight protected areas:

1. Political Affiliations;
2. Mental and psychological problems of the student or the student's family;
3. Sex behaviors and attitudes;
4. Illegal, antisocial, self-incriminating, or demeaning behavior;

GUIDANCE ON COLLEGE ADMISSIONS PRE-SURVEYS

FUTURE OF PRIVACY FORUM

FUTURE OF PRIVACY FORUM

TRAIN THE TRAINER

CIPA

FUTURE OF PRIVACY FORUM

FUTURE OF PRIVACY FORUM

TRAIN THE TRAINER

CHILDREN'S INTERNET PROTECTION ACT (CIPA)

The Internet safety policy adopted and enforced pursuant to 47 U.S.C. 254(h) must include a technology protection measure that protects against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by minors, harmful to minors. The school must enforce the operation of the technology protection measure during use of its computers with Internet access...This Internet safety policy must also include monitoring the online activities of minors.

Last updated: 2003

FUTURE OF PRIVACY FORUM

TRAIN THE TRAINER

COPPA

FUTURE OF PRIVACY FORUM

CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA)

- Creates rules around data collection from children under age 13.
- Enacted during the commercial/popular rise of the internet

FTC, Complying with COPPA: Frequently Asked Questions

COPPA APPLICABILITY

- Only applies to operators of commercial websites and online services (including mobile apps)
- Only applies to companies directly collecting information from children under age 13. If the operator doesn't do this, COPPA doesn't apply.
- Site/Service must 1) be directed to children, or 2) have "actual knowledge" that children <13 are using the site for the law to apply

COPPA REQUIREMENTS

- Companies subject to COPPA must obtain parental consent before collecting personal information from child, subject to narrow exceptions, and allow parents to withdraw consent if desired.
- If triggered, COPPA has specific requirements for collecting data and interacting with parents and children.

COPPA IN SCHOOLS

- When a school has contracted with an operator to collect PI from students solely for the benefit of students and school, the school can provide consent under COPPA
  - School consent applies solely for educational purposes

- Operator must:
  - Have a contract with the school, which addresses data collection, use, consent, etc.
  - Provide school with COPPA-required notices and rights
  - Maintain data for no longer than necessary to provide the educational service

WHY SHOULD DISTRICTS CARE ABOUT COPPA?

- COPPA considerations overlap FERPA school official considerations, as set forth in Department of Education guidance
  - PTAC guidance recommends that districts be aware of which online educational services are being used; have policies and procedures to evaluate and approve proposed online educational services; and evaluate written contracts and terms of service to confirm that they align with FERPA obligations

WHY SHOULD DISTRICTS CARE ABOUT COPPA?

- Some service providers may be more attuned to COPPA than FERPA
- Service contracts / terms of service / guidelines may contain provisions imposing obligations on schools to obtain COPPA consent
- Leverage?

QUESTIONS?

Amelia Vance
Director of Youth & Education Privacy
Future of Privacy Forum
avance@fpf.org

UPCOMING WEBINARS

MODULE 2: DEFINING DATA

SEA/LEA/CTE

Friday, April 17th 1-2 PM ET

Michael Hawes, *Senior Advisor for Data Access and Privacy*, U.S. Census Bureau; *Former Director,* Student Privacy Policy Office, U.S. Department of Education

LAW

Thursday, April 30th 1-2 PM ET

Kelsey Finch, *Senior Counsel*, Future of Privacy Forum

David Rubin, *Attorney at Law*, David B. Rubin P.C.

UPCOMING WEBINARS

MODULE 3: USING DATA IN EDUCATION

Friday, May 22nd 3-4 PM ET

MODULE 4: SHARING DATA

Thursday, June 18th 2-3 PM ET

Mark Williams, *Partner*, *Co-Chair*, eMatters and Higher Education Practice Groups, Fagen Friedman & Fulfrost LLP

Resources

The Federal Role in Safeguarding Student Data

Areas for federal action recommended by a coalition of national organizations

High-quality education data—data that are timely and useful—empower students, parents, educators, local and state education leaders, and policymakers with the information they need to make better decisions to improve student achievement and success. That is something all students and families deserve.

We are a coalition of organizations and individuals that represent diverse policy perspectives and believe adamantly in the effective use of data to support student learning and success. We believe everyone who uses student information has a responsibility to maintain its privacy and security.

As our school systems move into the digital age, we believe that the federal government has a role in prioritizing student data privacy and security and building trust in the use of student information. We offer the following context to frame the discussion about what the federal government can do to support the education field in safeguarding student data. We have identified three broad areas for federal action that we agree upon, although each of us may have differing opinions on how best to implement them.

Data Matter to Meeting Our Education Goals

We have more useful and richer information than ever before that can be used to support teaching and learning. But educators, students, and families will not use this information to make decisions, personalize learning, and help students succeed if they do not trust that doing so is safe. Over the past year, states, districts, education and privacy organizations, and school service providers have demonstrated tremendous leadership in prioritizing the need to safeguard student information. These efforts have led to greater transparency about what data are collected and for what purposes, stronger privacy and security laws and policies, clearer governance of data, and more open communication across the field—especially with parents and teachers.

There is a critical federal role in complementing, supporting, and reinforcing these activities. **Federal action should continue to align and clarify student protections and build capacity throughout the field to protect student information.**

Existing federal laws including the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and the Children's Online Privacy Protection Act (COPPA) offer an important legal foundation for safeguarding student data. Information practices and technological capabilities have changed radically since each of them was enacted. The federal government should continue to provide a clear student data privacy and security framework and support for states, local school systems, and schools that have varying legal and technical capacity.

Potential Areas for Federal Action

We believe that with appropriate federal leadership and guidance, state and local leaders and especially those closest to students—teachers and principals—can be informed about how federal laws apply to activities in the classroom and can be empowered to use education data well and safeguard them. We propose the three general areas for federal action on the following page.

FEDERAL LAWS THAT PROTECT STUDENT INFORMATION

LEGISLATION	DATE ENACTED	ADMINISTERED BY
Family Educational Rights and Privacy Act (FERPA)	1974	US Department of Education
Protection of Pupil Rights Amendment (PPRA)	1978	US Department of Education
Children's Online Privacy Protection Act (COPPA)	1998	Federal Trade Commission
Student Digital Privacy and Parental Rights Act	Expected in 2015	Federal Trade Commission

1. ENSURE THAT FEDERAL LAWS PROVIDE A STRONG FOUNDATION TO PROTECT STUDENT INFORMATION IN A CONSTANTLY CHANGING AND INCREASINGLY DIGITAL SCHOOL ENVIRONMENT.

THE CURRENT LANDSCAPE: Current federal laws do not specifically address current and evolving technology-driven practices that have implications for the privacy and security of student information. Student data are now collected, stored, and shared digitally—rather than on paper—often in cloud-based systems. New technologies can produce more sophisticated feedback on student progress and are informing classroom practices and educators' efforts to personalize instruction. While COPPA addresses online privacy, how the law applies to the use of various technologies in the classroom is not always clear to school districts and educators. And while FERPA has been applied to electronic records in some situations, the law is not designed to cover data collected outside of a student's official school record. Neither law addresses current and potential security concerns related to the aforementioned new digital capabilities.

THE FEDERAL ROLE: Federal law should establish a strong privacy and security foundation for educational institutions and agencies that provides baseline protections and consistency across states. Yet federal law should be broad enough to allow states and districts to innovate and respond to new developments in technology. Any changes to FERPA should recognize the electronic environments in which student data are generated and stored, account for schools' uses of third-party online applications that collect student information, and address the need for security safeguards designed for modern digital environments.

2. ENSURE THAT THE FEDERAL GOVERNMENT COORDINATES ACROSS AGENCIES TO PROVIDE CLARITY TO THOSE ON THE GROUND AS TO HOW PRIVACY LAWS WORK TOGETHER.

THE CURRENT LANDSCAPE: States and districts must navigate the student data privacy protections offered by federal laws, namely FERPA and PPRA, which are administered by the US Department of Education (ED), and COPPA, which is administered by the Federal Trade Commission (FTC). An aligned federal foundation that is coherent across applications and a continued commitment to coordinated communications can provide consistent definitions and standards for those on the ground.

THE FEDERAL ROLE: ED and the FTC should continue to coordinate to meet the needs of families, educators, and others working in states and school systems. These agencies can issue joint guidance to help individuals in states and districts navigate and implement federal privacy laws and inform complementary state laws and policies. They can help clarify for the public which federal laws govern student data privacy, their application in school settings, and federal governance of websites and online applications.

3. SUPPORT STATE AND LOCAL CAPACITY TO SAFEGUARD DATA.

THE CURRENT LANDSCAPE: To safeguard student data, individuals in schools and local school systems need training and support to build a culture of trust and implement best practices in data privacy and security. The federal government has numerous tools to support local infrastructure and capacity building. Federal agencies have already taken steps to support the field; the Privacy Technical Assistance Center, for example, has provided great value to the field through its hotline and its guidance on such important issues as data breach response and model terms of service.

THE FEDERAL ROLE: Continued federal attention to the role of states and school districts in safeguarding student data is vital. The federal government can do more to support them by providing more tools and resources to help them adopt policies and best practices in transparency, governance, and privacy and security. These supports can also include funding for building capacity—especially through related training and professional development—throughout the system, from the state to the local, school, and classroom levels. There are opportunities in federal law, such as the Elementary and Secondary Education Act, to address the need to equip teachers and school leaders to protect and use data effectively.

We, the undersigned organizations, support the three areas for federal action in safeguarding student data outlined in this document:

AASA, The School Superintendents Association

Alliance for Excellent Education

Association of Educational Service Agencies

Consortium for School Networking

Data Quality Campaign

The Education Trust

Future of Privacy Forum

International Association for K-12 Online Learning

International Society for Technology in Education

National Association of Elementary School Principals

National Association of Secondary School Principals

National Association of State Boards of Education

National Association of State Directors of Teacher Education and Certification

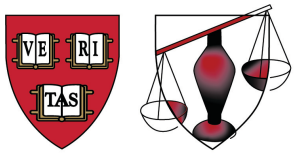
National Rural Education Advocacy Coalition

SIF Association

State Education Technology Directors Association

StriveTogether

StudentsFirst



Research Publication No. 2013-23
November 2013

Privacy and Children's Data - An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act

Dalia Topelson
Christopher Bavitz
Ritu Gupta
Irina Oberman

23 Everett Street • Second Floor • Cambridge, Massachusetts 02138
+1 617.495.7547 • +1 617.495.7641 (fax) • http://cyber.law.harvard.edu •
cyber@law.harvard.edu

STUDENT PRIVACY INITIATIVE
Berkman Center for Internet & Society

CYBERLAW CLINIC
Harvard Law School | Berkman Center for Internet & Society

PRIVACY AND CHILDREN'S DATA

An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act

November 2013

Dalia Topelson, Christopher Bavitz,
Ritu Gupta, and Irina Oberman

Berkman
The Berkman Center for Internet & Society
at Harvard University

23 Everett Street • Second Floor
Cambridge, Massachusetts 02138 • +1.617.495.7547
www.cyber.law.harvard.edu/research/studentprivacy

ACKNOWLEDGMENTS

Dalia Topelson is a Clinical Instructor at Harvard Law School's Cyberlaw Clinic, based at the Berkman Center for Internet & Society, and a Lecturer on Law at Harvard Law School. Christopher Bavitz is the Clinic's Managing Director and a Clinical Instructor and Lecturer on Law at HLS. Ritu Gupta and Irina Oberman were students in the Cyberlaw Clinic during the spring semester, 2013.

This guide was produced in advance of the Student Privacy Initiative's April 2013 workshop, "Student Privacy in the Cloud Computing Ecosystem," and is a product of the Harvard Law School's Cyberlaw Clinic. The Clinic provides high-quality, pro-bono legal services to appropriate clients on issues relating to the Internet, new technology, and intellectual property. Students enhance their preparation for high-tech practice and earn course credit by working on real-world litigation, client counseling, advocacy, and transactional / licensing projects and cases.

The Berkman Center for Internet & Society's Student Privacy Initiative explores the opportunities and challenges that may arise as educational institutions consider adopting cloud computing technologies. In its work across three overlapping clusters – Privacy Expectations & Attitudes, School Practices & Policies, and Law & Policy – this initiative aims to engage diverse stakeholder groups from government, educational institutions, academia, and business, among others, to develop shared good practices that promote positive educational outcomes, harness technological and pedagogical innovations, and protect critical values.

The Berkman Center is Harvard's university-wide center dedicated to the exploration, study, and development of cyberspace. The Center draws upon a vast network of faculty, students, entrepreneurs, lawyers, and virtual architects to diagnose both the opportunities and the challenges of cyberspace, particularly with regard to the need for legal structures.

The Clinic thanks Berkman Center Executive Director Urs Gasser, Project Manager Alicia Solow-Niederman, and Project Coordinator Shannon Walker for their help and input in developing this guide.

INTRODUCTION

Privacy law in the United States is a complicated patchwork of state and federal caselaw and statutes. Harvard Law School's Cyberlaw Clinic, based at the Berkman Center for Internet & Society, has prepared this briefing document to provide a high-level overview of two of the major federal legal regimes that govern privacy of children's and students' data in the United States: the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act.

The purpose of this document is to provide schools, parents, and students alike with an overview of some of the laws that may apply as schools begin to use cloud computing tools to help educate students. Both of the relevant statutes – and particularly FERPA – are complex and are the subjects of large bodies of caselaw and extensive third-party commentary, research, and scholarship. This document is not intended to provide a comprehensive summary of these statutes, nor privacy law in general, and it is not a substitute for specific legal advice. Rather, this guide highlights key provisions in these statutes and maps the legal and regulatory landscape.

Cloud computing is any functionality hosted on a network of remote servers that is available over the Internet. This can mean anything from an email service to full-fledged technology infrastructure, such as remote digital storage and remote computing power. Cloud computing also includes "software as a service," which allows one to access a computer program over the Internet.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

Overview

Congress enacted the Family Educational Rights and Privacy Act ("FERPA")[1] in 1974 to protect children's informational privacy and family privacy. FERPA prohibits the federal funding of educational institutions – schools, districts, and state education agencies – that release educational records to unauthorized persons.[2]

To whom does FERPA apply?

FERPA applies to public and private "educational agenc[ies] or institution[s]" that receive funds through particular programs administered by the United States Secretary of Education, who heads the Department of Education ("DOE").[3] The institution may receive federal funding either (1) directly, through grants, cooperative agreements, contracts, sub-grants, or sub-contracts;[4] or (2) indirectly, from students who receive scholarships or other funding from federal programs such as the Pell Grant Program or the Guaranteed Student Loan Program.[5]

What qualifies as an educational agency or institution?

Under FERPA, an educational agency or institution is defined as any school, district, or state education agency that: (1) receives federal funding (as described above), and

(2) either provides educational services or instruction to students or directs and controls public elementary, secondary, or post-secondary institutions.[6]

What information does FERPA protect?

FERPA protects the confidentiality of ***"education records."***

What qualifies as an "education record?"

Education records include any records, files, documents, or other materials that are "maintained by an educational agency or institution or by a person acting for such agency or institution" and contain information directly related to a student.[7] A "person acting for" the educational agency generally refers to agents of the school, such as teachers, administrators, and other school employees.[8] The Supreme Court has also stated that a person cannot be "acting for" an agency unless he or she also "maintains" the record.[9] Accordingly, peer-graded student papers and some student papers and tests that are briefly held for correction and grading alone are unlikely to be considered to be "maintained" by an education institution or a person acting for an educational institution.[10]

What information is not considered an "education record"?

The following are not considered "education records" under FERPA.[11]

- records that are made by faculty and staff for their own use as reference or memory aids and not shared with anyone other than a temporary substitute;[12]
- records of an educational agency or institution's law enforcement unit;[13]
- records of employees of an educational agency or institution that are made during the normal course of business and relate exclusively to their employment;[14]
- records of students 18 years or older or attending a post-secondary school that are created by professionals, such as physicians or psychiatrists, for treatment purposes;[15]
- records created by an educational agency or institution after an individual is no longer in attendance that do not directly relate to the individual's attendance as a student;[16] or
- grades on peer-graded papers before a teacher collects and records them.[17]

What are the rights of parents and eligible students under FERPA?

FERPA provides parents with certain rights to both protect and access their children's education records. These rights are transferred to students when they reach the age of eighteen or when they attend a post-secondary school.[18]

FERPA provides parents with four basic rights:

- the right to inspect and review educational records;[19]
- the right to challenge the content of education records and to correct or delete inaccurate, misleading, or inappropriate data;[20]
- the right to control the disclosure of education records containing their child's personally identifiable information via consent;[21] and
- the right to file a complaint regarding non-compliance of FERPA with the Department of Education (DOE).[22]

What are educational institutions' obligations under FERPA?

1. **Obtain parental consent**

   FERPA requires educational institutions to acquire parental consent prior to disclosing ***personally identifiable information*** from a student's education records, subject to some exceptions detailed below.[23] Personally identifiable information includes:[24]

   - the name of a student or a student's family member;
   - the address of the student or student's family members;
   - personal identifiers (*e.g.*, social security numbers and biometric records such as fingerprints, facial characteristics, or handwriting);
   - indirect identifiers (*e.g.*, date of birth, place of birth, mother's maiden name);
   - other information that, either alone or in combination, would allow a "reasonable person in the school community" to identify the student with reasonable certainty; and

- information that is requested by a person the institution reasonably believes knows the identity of the student.

The consent must be written and must be signed and dated by the parent. It must also specify the following:

- the records to be disclosed;
- the purpose of disclosure; and
- the parties to whom the disclosure is made.[25]

Consents may be signed electronically, as long as: (1) the mechanism by which the electronic signature is received identifies and authenticates a particular person as the source of the consent; and (2) the record of the consent indicates that person's approval of the information in the consent. Educational institutions must use "reasonable methods" to authenticate the source of a particular consent.[26]

2. **Notify parents and eligible students of their rights**

Educational institutions must ***inform*** parents and eligible students annually of their right:

- to inspect and review educational records;[27]
- to seek amendment of records;[28]
- to consent to disclose personally identifiable information;[29] and
- to file complaints with the DOE if the educational institution violates these provisions.[30]

The annual notice must also include the procedures that parents of eligible students must follow to review and amend documents.[31] The educational institution must deliver the annual notice in a format that is reasonably likely to ensure that the parents or eligible students are aware of their rights. This means that schools may need to create special notices to accommodate parents with disabilities or who are not native English speakers.[32]

3. **Maintain records of requests for access to and disclosure of personally identifiable information**

   Educational institutions must keep a record of each request for, and each disclosure of, personally identifiable information that is contained in a student's education records.[33] Educational institutions do not have to maintain records of disclosures made to the parent or eligible student, a school official, a party that has obtained written consent from the parent or eligible student, or a party that receives the information pursuant to a subpoena or other court order.[34]

   The record for each request or disclosure must include:

   - the names of parties that requested or received personally identifiable information from education records and any other parties to whom the information will be redisclosed;[35]
   - the parties' "legitimate interests" in requesting or obtaining such information;[36] and
   - the names of state and local education authorities and federal officials and agencies that may further disclose personally identifiable information from education records without consent.[37]

When can educational institutions disclose information without obtaining consent?

FERPA allows schools to disclose information without obtaining consent with respect to the following categories of information:

- student directory information;
- de-identified information; and
- in limited circumstances, personally identifiable information (as described below).

Schools may disclose ***student directory information*** without consent, as long as the schools ***notify*** parents and eligible students about the disclosure and provide parents and eligible students with a ***reasonable*** window during which they can opt out of the disclosure.[38] Directory information generally includes: name; address; telephone listing; e-mail address; photograph; date and place of birth; major; grade level; enrollment status; dates of attendance; degrees; honors and awards; most recent educational institution attended; and participation in sports and other activities.[39]

Directory information does *not* include social security numbers or student ID numbers.[40]

Schools may disclose ***de-identified data*** without prior parental consent. De-identification requires:

- removal of all personally identifiable information and
- a reasonable determination that a student's identity is not personally identifiable.[41]

Schools may disclose de-identified education records for education research purposes, provided that the school attaches a code to the de-identified data to allow the recipient of the data to match information received from the same source. This code must not be based on the student's social security number or other personal information, nor should it contain any information that would allow the recipient to identify a student based on the code.[42]

Schools may disclose ***personally identifiable information*** without prior parental consent to the following parties and in the following circumstances:[43]

- to school officials with "legitimate educational interests," including the "educational interests of the child for whom the consent would otherwise be required;"[44]
- to a contractor, consultant, or volunteer or to another entity to which the institution has outsourced institutional services if:
    - the educational institution would otherwise use its own employees for those services;
    - the entity is under the direct control of the institution in using and obtaining education records; and
    - the entity does not redisclose such information without parental consent;[45]
- to officials of another school where a student is transferring;[46]
- to specified officials for audit or evaluation purposes;[47]
- to determine financial aid for a student;[48]

Cloud computing service providers may be considered **school officials** if they are performing "institutional services" that would otherwise be performed by the school internally. Whether a cloud computing service provider would fall under this exception depends on who controls the service provider and how the service provider uses the student data it is processing. Simply including a contractual provision stating that the service provider is a "school official" is not enough. The service provider must manage the data as if it were the school itself to obtain education records without parental consent.

- to organizations conducting certain studies for or on behalf of the school;[49]
- to comply with a judicial order or lawfully issued subpoena, perpetration of a crime, or disciplinary proceeding;[50]
- to appropriate officials in cases of emergency to protect the health and safety of the student or other individuals;[51]
- to state and local authorities, within a juvenile justice system, pursuant to specific state law;[52] or
- to accrediting organizations.[53]

Additional resources about FERPA

- http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- http://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpafaq.pdf
- http://www2.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf
- http://ptac.ed.gov/

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Overview

The Children's Online Privacy Protection Act[54] and the Children's Online Privacy Protection Rule[55] (collectively, "COPPA") set forth privacy standards and obligations for online service providers that either target children or knowingly collect personal information from children under the age of 13.

To whom does COPPA apply?

COPPA applies to operators of websites or online services.

Who or what qualifies as an operator?

An operator is any individual or entity that either:

- operates a commercial website or online service ***directed to children*** under thirteen years of age that collects personal information from children; or

- operates a ***general audience website*** and has actual knowledge that it collects personal information from children under thirteen years of age.[56]

How does one determine if a website or online service is directed to children?

The Federal Trade Commission (FTC) considers a number of factors to determine whether a site or service is "directed to children," including the:[57]

- subject matter;
- visual or audio content;
- age of models;
- language or other characteristics;
- whether advertising promoting or appearing on the site is directed to children;
- empirical evidence regarding audience composition;
- intended audience; and
- whether a site uses animated characters and/or child-oriented activities and incentives.

Do non-profits or government agencies or institutions have to comply with COPPA?

An Operator as defined by COPPA "does not include any nonprofit entity that would otherwise be exempt from coverage under the Federal Trade Commission Act."[58] Section 5 of the Federal Trade Commission Act (the "FTC Act") and accordingly, the FTC's enforcement jurisdiction, only applies to "persons, partnerships, or corporations."[59] A "corporation" is defined as an entity that "is organized to carry on business for its own profit or that of its members."[60] Therefore, non-profit entities or entities that are not "corporations" (such as government agencies) are generally not subject to the FTC's jurisdiction, and accordingly are not required to comply with COPPA.[61]

According to the FTC, however, non-profit entities that operate websites or services for the profit of their commercial members may be subject to liability under COPPA.[62] Schools generally do not qualify as commercial institutions that are subject to the jurisdiction of the FTC. That said, if a school engages in commercial activity

(for instance, selling t-shirts online), then that behavior could be subject to oversight by the FTC.

Likewise, even if a school is not subject to FTC oversight, the cloud computing service providers that schools engage are likely to be subject to the FTC's jurisdiction. To that end, any time a school engages a cloud computing service provider, it should ensure that the service provider complies with COPPA.

To what types of data does COPPA apply?

COPPA applies to ***any personal information collected from children under the age of 13***. Personal information includes: first and last name; a home or other physical address; an e-mail address; a telephone number; a social security number; photos, videos, or audio files that contain a child's image or voice; geolocation information; a persistent identifier that can be used to recognize a user over time and across different websites or services; and any other information that permits the physical or online contacting of a specific individual.[63]

Although COPPA protection only applies to children under 13, the FTC encourages operators to protect information collected from teenagers aged 13 and over as well.

Does COPPA apply to information collected from parents?

While COPPA does not generally apply to personal information collected from parents about their children, as a best practice, operators should safeguard information obtained from parents in the same way that they would if collected directly from a child. At a minimum, operators are expected to maintain the confidentiality of information collected from parents when parents provide consent for the release of their child's information or when they review information collected from their child.[64]

What does it mean to "collect" data under the statute?

COPPA applies to both ***active and passive data collection***. Active collection occurs when an operator directly solicits information from children or enables children to make their personal information available through chat rooms and message boards.[65] Passive data collection involves the tracking or use of "any identifying code linked to an individual, such as a cookie," as well as any other "identifiers" that can be used to identify, contact, or locate a child over time and across different websites or online services.[66]

What are website operators' obligations under COPPA?

1. **Provide notice to parents**

   An operator must make "reasonable efforts" to ensure that parents receive ***notice*** of a ***website or online service's collection, use, and disclosure*** of their child's personal information.[67]

   The content of the parental notice must include all of the content that COPPA requires an operator to disclose in its privacy policy. Additionally, it must state:[68]

   - that the operator wishes to collect information from a particular child;
   - the type of information an operator wishes to collect;
   - the purpose of information collection; and
   - the means by which parents can provide and revoke consent, where verifiable parental consent is required.[69]

2. **Obtain parental consent**

   When must an operator obtain verifiable parental consent?

   An operator must obtain verifiable parental consent ***prior*** to ***collecting, using, or disclosing any child's personal information***. An operator must also obtain verifiable parental consent any time its collection, use, or disclosure practices "materially change," even if the operator has already obtained consent from the parent.[70] For instance, if an operator has obtained parental consent to share a child's personal information to third-parties for a particular purpose, and that purpose changes, then the operator must obtain a new consent to use or share the information for the new purpose.

   When is prior parental consent not required?

   An operator can collect a child's name or online contact information prior to obtaining parental consent where it collects such information:[71]

   - solely to provide direct notice and obtain parental consent;
   - to respond to a child's specific request on a one-time basis;[72]

- to send the child periodic communications, including online newsletters, site updates, or password reminders;[73]

- as reasonably necessary to protect the safety of a child participant on the website; or

- to protect the website's integrity, take precautions against liability, respond to judicial process, or respond to an agency's request for a matter related to public safety.[74]

An operator may also disclose information collected from children without parental consent to corporate affiliates who: (1) solely provide internal support for the website or service; (2) are required to keep the information confidential and are restricted from using the information for any other purpose, and (3) play no role in collecting, maintaining, or using the personal information collected from children through the service.[75]

How can an operator obtain parental consent?

Any method of obtaining verifiable parental consent must be "reasonably calculated, in light of available technology," to ensure that the consent is being given by a child's parent.[76] For example:

- For ***solely internal*** uses of personal information (not disclosed to third-parties and not publicly available), the FTC recommends that operators seek parental consent through an e-mail from a parent, followed by sending a confirmatory consent via postal mail, facsimile, or telephone call. In the event of a "reasonable time delay," an operator can send another email to verify that the parent has given consent.[77]

- If personal information is ***publicly disclosed*** (such as via chat rooms or message boards) or disclosed to third-parties, the FTC recommends obtaining parental consent in a variety of ways that attempt to verify the parent's identity, such as:

    - providing a consent form for parents to sign and send back via mail, fax, or electronically;

    - requiring a parent to use a credit card in a secured transaction;

    - maintaining a toll-free telephone number staffed by trained professionals where parents can call in their consent;

- an email with a digital signature;
- an email with a PIN or password obtained through one of the prior methods; or
- using government-issued identification, such as a driver's license.[78]

- COPPA permits a school to obtain parental consent on the operator's behalf, as long as the operator uses the information only on behalf of the school pursuant to the agreement between the school and the operator.[79] While an operator can presume that schools have obtained parental consent for any personal information they disclose to the operator, it must comply with the boundaries of the consent obtained by the school.[80] An operator must obtain consent directly from the parents if it wants to use the data collected from the school for its own commercial purposes.[81]

3. **Manage disclosures to third-parties**

Operators must take reasonable steps to ensure that a child's personal information is disclosed only to those third-parties who will maintain the confidentiality, security, and integrity of the information.[82] To that end, operators should conduct due diligence on any third-parties they plan to share information with, and should only share a child's personal information with trusted parties that are contractually bound to maintain the "confidentiality, security, and integrity" of such information.[83]

4. **Maintain a privacy policy**

Operators must maintain a privacy policy that is clear, easy to understand, complete, and does not contain extraneous information. The content of the privacy policy must include:[84]

- the names of *all operators* that collect or maintain personal information from children;
- the types of personal information collected and whether collection is active or passive;
- uses, or potential uses, of the information;
- disclosures and uses by third-parties;

- that parents may give limited consents to the collection and use of their child's personal information without consenting to its disclosure to third-parties;

- that an operator cannot condition a child's participation in an activity on his disclosure of more information than is "reasonably necessary"; and

- that a parent may review his or her child's personal information, request its deletion, and refuse to consent to further data collection.

Operators must provide ***effective notice of their privacy policies on their websites***. The link to the privacy policy must be clearly labeled and placed in a clear and prominent manner both on the home page and any other area where children provide, or are asked to provide, personal information.[85] A general audience websites must contain a link to the privacy policy on the homepage of the children's area of its website.[86] The FTC suggests using a larger font size, different color, or a contrasting background for emphasis.[87]

5. **Retention and disposal of personal information**

   COPPA requires operators to retain a child's personal information "for only as long as is reasonably necessary" and to protect against intrusions even when disposing of the information.[88] This allows operators to determine their own data retention and deletion capabilities, without the FTC dictating certain timeframes or destruction policies.

Does COPPA offer any safe harbors against liability?

In lieu of complying with COPPA's requirements, operators may submit a self-regulatory program to the FTC for approval.[89] If approved, the operator is offered a "safe harbor" from complying with COPPA's requirements as long as the operator complies with the self-regulatory program approved by the FTC.[90] For information about applying for FTC approval of a safe harbor program, see C.F.R. Section 312.11, http://www.business.ftc.gov/privacy-and-security/childrens-privacy, or email CoppaHotLine@ftc.gov.[91]

Additional resources about COPPA

- http://www.ftc.gov/ogc/coppa1.htm

- http://www.ftc.gov/os/fedreg/2013/01/130117coppa.pdf

- http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions
- http://www.ftc.gov/opa/2013/07/coppa.shtm
- http://business.ftc.gov/blog/2012/12/ftcs-revised-coppa-rule-five-need-know-changes-your-business
- http://business.ftc.gov/documents/bus84-childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business

ENDNOTES AND CITATIONS

[1] The Family Educational Rights and Privacy Act (FERPA), Pub. L. No. 93-380 (1974), codified at 20 U.S.C. § 1232g. The regulations that administer FERPA are incorporated in 34 C.F.R. § 99.

[2] 20 U.S.C. § 1232g; See also Gonzaga Univ. v. Doe, 536 U.S. 273, 276 (2002).

[3] 34 C.F.R § 99.1(a); See also Family Educational Rights and Privacy Act (FERPA), U.S. DEP'T OF EDU., http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (last visited Mar. 25, 2013).

[4] 34 C.F.R § 99.1(c)(1).

[5] Id. § 99.1(c)(2).

[6] Id. § 99.1.

[7] 20 U.S.C. § 1232g(a)(4)(A).

[8] See Owasso Independent School District v. Falvo, 534 U.S. 426, 433 (2002).

[9] Id. at 433–34.

[10] Id.

[11] 34 C.F.R. § 99.3("Education records")(b)(1); see also FERPA Frequently Asked Questions (FAQ), PA. STATE UNIV., http://www.registrar.psu.edu/confidentiality/FERPA_faq.cfm (last visited Mar. 25, 2013) [hereinafter PSU FAQs].

[12] 34 C.F.R. § 99.3("Education records")(b)(1).

[13] Id. § 99.3("Education records")(b)(2).

[14] Id. § 99.3("Education records")(b)(3).

[15] Id. § 99.3("Education records")(b)(4).

[16] Id. § 99.3("Education records")(b)(5).

[17] Id. § 99.3("Education records")(b)(6).

[18] *See* 20 U.S.C. § 1232g(d) ("whenever a student has attained eighteen years of age, or is attending an institution of postsecondary education, the permission or consent required of and the rights accorded to the parents of the student shall thereafter only be required of and accorded to the student"); see also 34 C.F.R. § 99.5 ("What are the rights of students?"); Frequently Asked Questions, U.S. DEP'T OF EDU., http://www2.ed.gov/policy/gen/guid/fpco/faq.html (last visited Mar. 25, 2013) [hereinafter FERPA FAQs].

[19] 20 U.S.C. § 1232g(a)(1)(A) (2006).

[20] Id. § 1232g(a)(1)(D)(2).

[21] Id. § 1232g(b)(2); 34 C.F.R. § 99.30(a).

[22] 34 C.F.R. §§ 99.7(a)(2)(iv), 99.63 and 99.64.

[23] Id. §§ 99.30(a) and 99.31.

[24] Id. § 99.3 ("Personally Identifiable Information").

[25] Id. § 99.30(b).

[26] Id. § 99.30(d).

[27] Id. § 99.7(a)(2)(i).

[28] Id. § 99.7(a)(2)(ii).

[29] Id. § 99.7(a)(2)(iii).

[30] Id. § 99.7(a)(1)(iv).

[31] Id. § 99.7(a)(3)(i)–(ii).

[32] Id. § 99.7((b).

[33] Id. § 99.32(a)(1).

[34] Id. § 99.32(d).

[35] Id. § 99.32(b)(1)(i)-(ii).

[36] Id. § 99.32(b)(1)(i)-(ii)

[37] Id. § 99.32(a)(1).

[38] 20 U.S.C. § 1232g(a)(5)(B) (2006).

[39] FERPA FAQs, supra note 18.

[40] 34 CFR § 99.3 ("Directory information")(b)(1)-(2).

[41] Id. § 99.31(16)(b)(1).

[42] Id. § 99.31(16)(b)(2).

[43] Id. § 99.31(a).

[44] Id. § 99.31(a)(1)(i)(A); 20 U.S.C. § 1232g(b)(1)(A) (2006).

[45] 34 C.F.R. § 99.31(a)(1)(i)(B).

[46] Id. § 99.31(a)(2); id. § 99.34(a)

[47] Id. § 99.31(a)(3)

[48] Id. § 99.31(a)(4).

[49] Id. § 99.31(a)(6)(i).

[50] Id. § 99.31(13)–(16).

[51] Id. § 99.36(a).

[52] 20 U.S.C. § 1232g(a)(5)(E) (2006).

[53] Id. § 1232g(a)(5)(G).

[54] 15 U.S.C. §§ 6501- 6506 (1998)

[55] 16 C.F.R. § 312 (2013).

[56] 15 U.S.C. § 6501(2); 16 C.F.R. § 312.2 (2013).

[57] See 16 C.F.R. § 312.2 (2013) (definition of "Website or online service directed to children").

[58] 16 C.F.R. § 312.2 ("Operator") (2013).

[59] 15 U.S.C. § 45.

[60] Id. at § 44.

[61] See 15 U.S.C. § 6501(2)(A) (1998) (defining "operator" as one who operates a website where the website is "operated for commercial purposes"); id. § 6501(10)(A) (defining a "website or online service directed to children" as a "commercial website or online service that is targeted to children" or portion thereof); see also Complying with COPPA: Frequently Asked Questions, FED. TRADE COMM'N (last revised July 2013) [hereinafter COPPA FAQs].

[62] See FTC v. Cal. Dental Ass'n, 526 U.S. 756 (1999); see also COPPA FAQs supra note 61, Question B(5); see also 15 U.S.C. § 45.

[63] 16 C.F.R. § 312.2 ("Personal information") (2013).

[64] See 64 Fed. Reg 59,888, 59,902 n.213 ("The Commission expects that operators will keep confidential any information obtained from parents in the course of obtaining parental consent or providing for parental review of information collected from a child.").

[65] 16 C.F.R. § 312.2 (2013).

[66] See Press Release, Fed. Trade Comm'n, FTC Strengthens Kids' Privacy Gives Parents Greater Control Over Their Information By Amending Children's Online Privacy Protection Rule (Dec. 19, 2012), http://www.ftc.gov/opa/2012/12/coppa.shtm [hereinafter FTC Press Release] (emphasis added).

[67] 16 C.F.R. § 312.4

[68] Id.

[69] Id.

[70] Id. § 312.5(a).

[71] 16 C.F.R. § 312.5(c).

[72] Id. § 312.5(c)(3); See also 78 Fed. Reg. 3972, 3993 (Jan. 17, 2013).

[73] 16 C.F.R. § 312.5(c)(4); See also 78 Fed. Reg. 3972, 3993 (Jan. 17, 2013).

[74] Id. § 312.5(c)(5).

[75] COPPA FAQs, supra note 61, Questions I(6) - I(10).

[76] 16 C.F.R. § 312.5(b). See also COPPA FAQs, supra note 61, Questions C(11) and C(12).

[77] Id.

[78] Id.

[79] COPPA FAQs, supra note 61, Questions M(1) - M(3)

[80] Id.

[81] Id.

[82] 16 C.F.R. 312.8

[83] Id.; See also COPPA FAQs, supra note 61, Questions M(2) - M(3).

[84] 16 C.F.R. § 312.4(d).

[85] Id.

[86] Id.

[87] COPPA FAQs, supra note 61, Question C(8).

[88] 16 C.F.R. § 312.10

[89] Id. § 312.11

[90] Id. § 312.11(g).

[91] COPPA FAQs, supra note 61, Questions N(1) - N(3).

PROGRAMS

Family Educational Rights and Privacy Act (FERPA)

Get the Latest on FERPA at https://studentprivacy.ed.gov/

- **Frequently Asked Questions**
- FERPA for **parents and students**, **K12 school officials** and **Postsecondary school officials**
- Protection of Pupil Rights Amendment (**PPRA**)
- **Guidance and Notices**

Family Policy Compliance Office (FPCO) Home

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
  - School officials with legitimate educational interest;
  - Other schools to which a student is transferring;
  - Specified officials for audit or evaluation purposes;
  - Appropriate parties in connection with financial aid to a student;
  - Organizations conducting certain studies for or on behalf of the school;
  - Accrediting organizations;
  - To comply with a judicial order or lawfully issued subpoena;
  - Appropriate officials in cases of health and safety emergencies; and
  - State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

For additional information, you may call 1-800-USA-LEARN (1-800-872-5327) (voice). Individuals who use TDD may use the Federal Relay Service.

Or you may contact us at the following address:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-8520

Last Modified: 03/01/2018

How Do I Find...

- Student loans, forgiveness
- College accreditation
- Every Student Succeeds Act (ESSA)
- FERPA
- FAFSA
- 1098, tax forms

More >

Information About...

- Transforming Teaching
- Family and Community Engagement
- Early Learning

Related Topics

- **No Related Topics Found**

Children's Privacy

The Children's Online Privacy Protection Act (COPPA) gives parents control over what information websites can collect from their kids. The COPPA Rule puts additional protections in place and streamlines other procedures that companies covered by the rule need to follow. The COPPA FAQs can help keep your company COPPA compliant. Learn about the COPPA Safe Harbor Program and about organizations the FTC has approved to implement safe harbor programs. You can also get information about ways to get verifiable parental consent– including new methods the Commission has approved – and the process for seeking approval for new methods.

FEATURED

Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business

A step-by-step plan for determining if your company is covered by COPPA — and how to comply with the Rule.

GUIDANCE

Children's Online Privacy Protection Rule: Not Just for Kids' Sites

The Children's Online Privacy Protection Act (COPPA) applies to websites for kids, but it also may apply to sites aimed at general audiences. Read this revised publication to find out when your site is subject to COPPA.

Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business

A step-by-step plan for determining if your company is covered by COPPA — and how to comply with the Rule.

Complying with COPPA: Frequently Asked Questions

Need resources on the Children's Online Privacy Protection Rule? These revised FAQs from the FTC can help keep your company COPPA compliant.

Related Posts

FEB 25, 2020
FTC's Privacy & Data Security Update for 2019 – and how you can use it

JAN 8, 2020
FTC consumer protection year in review offers 2020 vision for your business

DEC 10, 2019
COPPA comment deadline extended to December 11th

NOV 22, 2019
YouTube channel owners: Is your content directed to children?

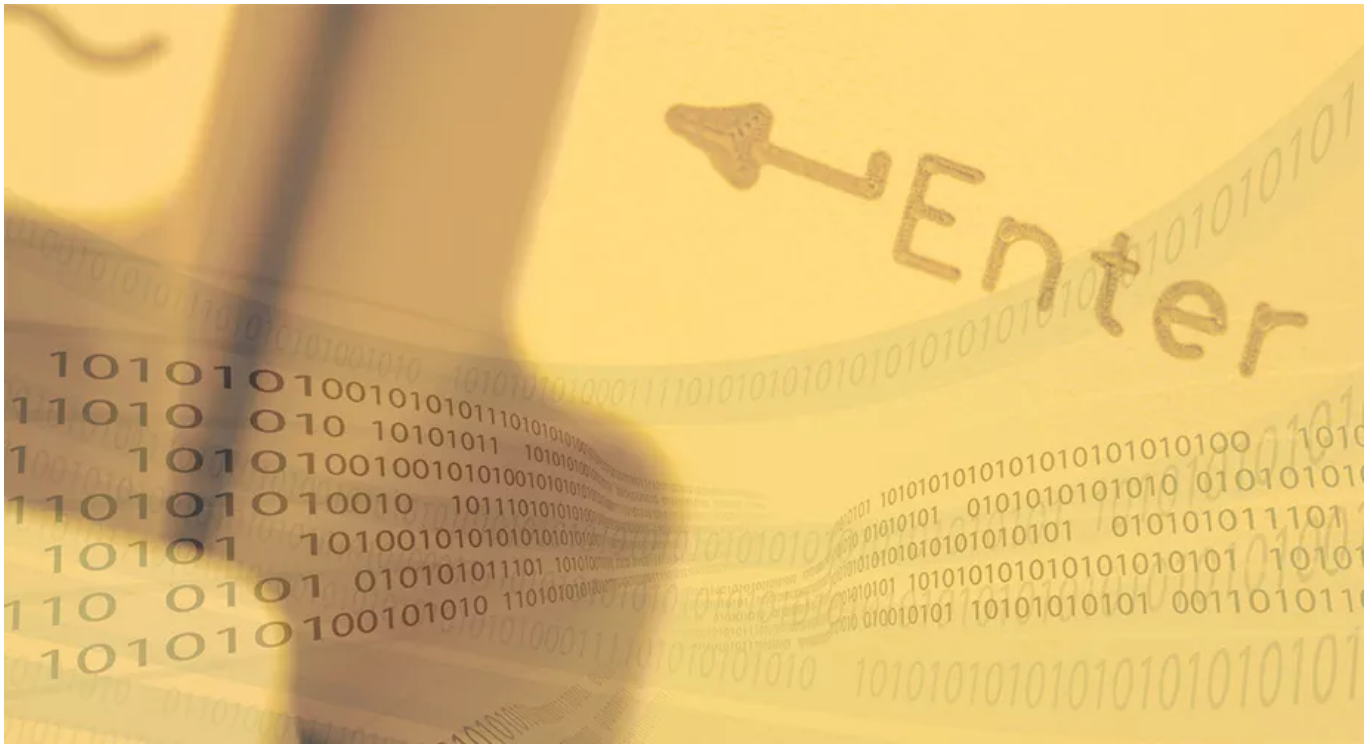
OCT 22, 2019
FTC takes action against stalking apps

Legal Resources on Children's Privacy

Case (33)
Press Release (17)
Closing Letter (15)
Public Statement (13)
Report (9)
Public Event (6)
Federal Register Notice (5)
Rule Summary (1)
Public Comment Initiative (1)

Published: July 28, 2017

COPPA and Schools: The (Other) Federal Student Privacy Law, Explained



By Benjamin Herold

When it comes to federal protections for students' sensitive personal information, the Family Educational Rights and Privacy Act, or FERPA, tends to get most of the attention.

But schools also need to be familiar with the **Children's Online Privacy Protection Act**, commonly known as COPPA.

In a nutshell, COPPA requires operators of commercial websites, online services, and mobile apps to notify parents and obtain their consent before collecting any personal information on children under the age of 13. The aim is to give parents more control over what information is collected from their children online.

This law directly regulates companies, not schools. But as the digital revolution has moved into the classroom, schools have increasingly been put in the middle of the relationship between vendors and parents.

The Federal Trade Commission, which enforces COPPA, has said that schools can, in many situations, stand in for parents and let companies collect information from young children. In some cases, companies may try to shift some of the burden of COPPA compliance away from themselves and onto schools. And it's clear that the law places significant indirect burdens on schools and educators.

Jump to a Section

Those dynamics have opened up multiple cans of worms, said Sonja H. Trainor, the director of the Council of School Attorneys for the National School Boards Association.

> **What Are the Penalties for COPPA Violations?**

"The FTC has decided, not based on law or regulation, but as a practical reality, that schools can give consent on behalf of parents," Trainor said. "That is not without risk, and COPPA has a whole lot of gray area that gives school attorneys pause."

In an emailed response to questions from *Education Week*, FTC staff members provided clarification and new insights on a number of key areas that have had both schools and vendors worried.

But despite whispers in the field that the Federal Trade Commission and the U.S. Department of Education may be gearing up to jointly issue a formal new document with more answers, the commission doesn't "currently have a timetable for release of additional business guidance," according to FTC staff.

In the meantime, what do school boards, superintendents, principals, teachers, parents, and companies serving the K-12 market need to know?

Education Week turned to federal officials and documents, education law experts, and leaders in the field of student-data privacy to get their advice.

What exactly is COPPA?

The Children's Online Privacy Protection Act was enacted by Congress in 1998. The law requires the Federal Trade Commission to "issue and enforce regulations concerning children's online privacy," according to the **FTC's frequently-asked-questions page** (which you might want to bookmark).

The commission put its first COPPA-related rules in place in 2000, and **amended them in 2013**.

Who does COPPA apply to?

Two groups:

Operators of commercial websites, online services, and mobile apps that are directed at children under 13 and "collect, use, or disclose personal information" from those kids.

And operators of websites and online services that are for a general audience but have "actual knowledge" that they are collecting, using, or disclosing personal information from children under 13.

COPPA generally does not apply directly to state government agencies, schools, or nonprofits.

What does COPPA require companies to do?

The list is long. Among other things, COPPA-covered operators must:

- Post a "clear and comprehensive" online-privacy policy
- Give parents "direct notice" before collecting information from children under 13
- Obtain "verifiable parental consent" before collecting such information
- Allow parents to review their children's information and request that it be deleted
- Allow parents to opt out of further collection, use, or sharing of information pertaining to their child
- Maintain the confidentiality and security of any child's information that is collected
- Delete children's information after it is "no longer necessary to fulfill the purpose for which it was collected."

What types of information are we talking about?

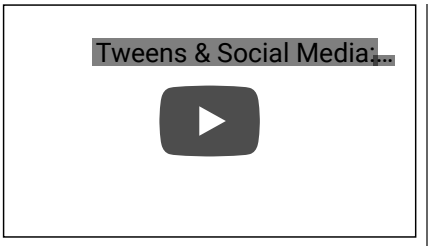
Video: Tweens & Social Media

For COPPA purposes, "personal information" can mean a child's name, address, or Social Security number; his or her username or screen name, if

that could be used to make contact with the child; some geolocation information; persistent identifiers that might allow the child to be tracked across time or across websites; and more.

Less clear, though, is whether COPPA covers information such as IP (internet protocol) address, device identification number, the type of browser being used, or other so-called metadata that can often be used to identify users.

It's worth noting that COPPA applies only to information that is collected *from* children, not to information that is collected *about* children. So services that collect information from parents, for example, are not covered, even if some of that information pertains to their children.



Schools are increasingly looking at teaching digital citizenship - the appropriate use of technology. It's a lesson some believe should start as young as elementary school. **View more ed-tech videos.**

OK, cut to the chase—where do K-12 schools come into the COPPA discussion?

Here's the heart of the matter:

In its FAQs, the Federal Trade Commission says that under certain circumstances, "schools may act as the parent's agent and can consent to the collection of kids' information on the parent's behalf."

There's a lot to unpack in that.

Yes, there is.

Let's start here: Do schools have to obtain parental consent to pass along to companies, or can schools grant consent in place of parents?

This is one of those big questions that have given schools pause. Trainor of the Council of School Attorneys, for example, said that some school lawyers have taken the FTC's previous guidance to mean that their districts must get consent from every single parent, for every single product that collects information online from young children.

In its responses to *Education Week*, though, the FTC provided new clarity.

"When schools give consent, the school may consent in lieu of the parents," according to staff at the commission.

That's what often already happens in practice, said Bill Fitzgerald, the director of privacy-evaluation initiatives at Common Sense Media.

But there are still a number of issues for schools to consider.

Whether and how schools can grant COPPA consent varies under certain circumstances, Fitzgerald said.

And in addition to consent, the law requires parental notification. Generally, the FTC expects companies to publicly post a privacy policy that includes descriptions of what information is collected from children, how that information may be used and disclosed, contact information for any third parties that may also be collecting information through the site, and more. Schools in turn are expected to make such notices available to parents. In practice, the details of that information exchange can get messy.

You said whether and how schools can grant COPPA consent varies under "certain circumstances." Explain.

First, according to the FTC, schools can grant consent on behalf of parents only when the operator of the website, online service, or app in question is providing a service that is "solely for the benefit of students and the school system" and is specific to "the educational context."

If the service isn't just for education, the operator and/or the school clearly has to get verifiable consent directly from parents.

How are schools supposed to determine if a website or app is strictly educational?

Now you're starting to see just how tricky this can get.

In its FAQs, the trade commission does provide a helpful list of questions for schools to ask operators when seeking to make this determination.

First and foremost, what information will be collected, and how will it be used?

And more specifically, will any information collected from children under 13 be used or shared for commercial purposes unrelated to education? Are schools allowed to review the information collected on students? Can schools request that student info be deleted?

If the answers to that second group of questions are, respectively, yes, no, or no, schools are not allowed to grant consent on behalf of parents, according to the FTC.

That sounds fairly straightforward.

In reality, it's not.

Fitzgerald of Common Sense Media laid out a number of areas where this can get complex.

In many cases, he said, companies include in their terms of service a provision that it's the school's responsibility to get verifiable consent from parents. Companies may even stipulate that schools using their service are required to retain proof of that consent and produce it on demand. If it's in the terms of service, it can be binding for schools that use the product, Fitzgerald said. The takeaway, he said, is that schools should read *carefully* all terms of service before letting students use a website, online service, or app.

Is that it?

No. Many vendors also allow third-party trackers (usually related to analytics or advertising) to be embedded into their sites and services. This complicates things tremendously, on all sides.

In its FAQs, the FTC says that operators are responsible for determining the "information-collection practices of every third party that can collect information" via their app, service, or site. And in response to questions from *Education Week*, FTC staff members went even further, writing that "generally speaking, an operator must disclose the existence of any third-party tracking services that are collecting personal information from children using the operator's website or online service."

In practice, though, vendors often don't provide that information to schools, or do so only in vague or conditional terms. In response to questions from *Education Week*, FTC staff said operators that don't adequately disclose the activity of third-party trackers that collect information from users under 13 cannot obtain informed consent from either parents or schools. That declaration could have huge implications.

Is *that* it?

Not quite. There's also a bigger reality that places schools in a bind when determining if and how they can grant COPPA consent on behalf of parents: Many of the online services in schools have both educational *and* commercial versions and applications.

Think about Google, for example. It's not at all unusual for students to enter one of G Suite's educational services through their student accounts, then venture out from there to one of Google's commercial services, like Maps or Search.

For years, Google has declined to provide detailed answers to questions about **exactly how it collects and uses information generated by students** in those circumstances—making it difficult for schools to determine for

COPPA purposes whether G Suite is strictly for the benefit of schools and students within the "educational context."

That must worry educators. Can schools be held liable for COPPA violations, or for improperly granting consent to a company that commits COPPA violations?

There are a number of ways to think about this.

First, here's how FTC staff responded when *Education Week* posed this exact question: "COPPA applies to operators of commercial websites and online services. COPPA does not apply to schools."

For Trainor of the Council of School Attorneys, though, the legal considerations for schools aren't quite so cut-and-dried. Here's what she had to say:

I wouldn't say the liability concerns for schools are so extreme that they should be put above more everyday concerns, like budgets or student achievement. But I would say that school leaders should be aware that this is a fuzzy area of the law. And school boards should be asking their attorneys and state board associations what kind of liability might exist in their state.

And then there's the broader issue of public trust and perception. If a school grants consent for an operator to collect information from young children, and that company turns around and violates COPPA, the school may not face any legal liability. But it's almost certain the school will have some angry parents to contend with.

OK, let's get practical for a second. *How* do schools notify parents and get their consent under COPPA?

Often through an Acceptable Use Policy or similar document that is sent home to parents at the beginning of the school year, said Fitzgerald of Common Sense Media. Sometimes, such a document describes the types of online services a school intends to use, what types of information they may collect, and how that information might be used. Even better, Fitzgerald said, is when schools provide a detailed list of exactly what websites/online services/apps students will be using, and what the information practices of each are.

This probably isn't as straightforward as it sounds, either.

Nope.

For one thing, some privacy experts say that a one-time, blanket sign-off at the beginning of the school year may not be considered valid notification and consent under COPPA, especially if it doesn't list the specific online services that children will be using.

Who in the school should be responsible for granting COPPA consent?

In its FAQs, the FTC recommends that this happen at the school or district level, and that responsibility for deciding "whether a particular site's or service's information practices are appropriate" not be delegated to teachers.

Many districts do in fact have that kind of review-and-approval process.

But don't many teachers also make their own decisions about what sites and apps they use?

Yes.

In fact, that's the **explicit business model** of a lot of ed-tech companies: Go around (often slow, tedious) district approval processes by marketing directly to teachers and hoping for viral growth.

But that presents a couple of problems.

One is “click-wrap agreements.” Often, these are the kinds of agreements that almost all of us are guilty of just clicking through without actually reading. Significantly, FTC staff said that “typically, a click-wrap agreement on its own would not suffice” to meet COPPA standards around notification and consent. This point could have big implications for both companies and schools.

More broadly speaking, it’s still unclear whether a teacher can enter into a contract and provide COPPA consent on behalf of parents, even if it’s not via a click-wrap agreement, said Amelia Vance, the education-privacy-policy counsel at the Future of Privacy Forum.

Many schools seek to avoid any situation where a teacher can incur liability on behalf of the district—and for good reason, she said.

“You just naturally have less due diligence when a teacher is the one signing up,” Vance said. “They have a million things to do in a day, and that doesn’t often include going through detailed privacy policies on a company’s website to verify that it’s in compliance with COPPA.”

Does consent for a child to use a site/service/app carry over from year to year, or do schools need to get fresh consent each school year?

This is yet another gray area that’s been troubling schools. The FTC provided some helpful insights to *Education Week*. Here’s what commission staff wrote in their response to our question:

The consent [granted by a parent or school under COPPA] is specific to the particular website or online service offered and is not tied to the specific class or school year. However, COPPA requires the provider of the site or service to obtain a separate consent for any material change to its data collection or use practices.

In practice, Fitzgerald said, this appears to mean that a parent or school granting a company consent to collect information online from a child “basically lasts forever.”

That would seem to be true even if the nature of the site or service evolves dramatically over time, Vance added.

What about when kids move?

In this situation, the new school enrolling the child “should ensure that it has received the necessary notice from the operator and given consent for the child’s use,” according to FTC staff.

In practice, Vance said, that appears to mean that COPPA consent is not transferable from school to school. That appears to be especially true when a child moves between states that may have different student-data-privacy laws of their own.

Vance also raised another question: When a child under 13 moves, what happens to the COPPA-covered information that companies hold on that child?

“The first thing parents do when they move is not go find all the companies who are storing their child’s information and make sure it’s deleted,” she said. “And there’s not really a clear process by which schools can go to companies and let them know a child is no longer there.”

Well, what’s the answer?

It’s not clear.

What happens when an operator collects information on a child under 13, and then that child turns 13?

According to FTC staff, COPPA does not require any new consent for newly collected personal information after a child turns 13.

Other privacy laws likely apply, though.

And FTC staff did have this to say, which again could have big implications for schools and ed-tech companies:

An operator cannot combine the previously collected personal information [from a child under 13] with the newly collected personal information [from the same child, once he or she is 13 or older], to engage in uses beyond what had previously been consented to by either parents or a school. And of course, any data collected from a child under 13 can only be retained as long as is reasonably necessary to fulfill the purpose for which the information was collected.

Let's say a school successfully and appropriately provides COPPA consent for its students to use a particular app. Do parents still retain their rights under the law?

Good question. Remember, COPPA isn't just about consent. It also requires operators to let parents review their children's information, request that it be deleted, and more.

Unfortunately, the FTC's response to *Education Week* didn't provide much clarity.

Trainor, the director of the school attorneys' group, said this is another gray area.

"I think parents might be able to make that request directly of an operator under COPPA," she said. "But it's fuzzy."

What about schools? Under COPPA, can they request to review/delete the information collected from children under 13? Should they? Does this ever happen?

Yes, it does happen, but probably not as often as it should, privacy advocates say.

Fitzgerald of Common Sense Media is among those who would "love to see schools and parents get together and submit sample requests" just to see what happens.

What are the penalties for COPPA violations?

Operators can be hit with a civil penalty of up to $40,654 per violation.

For companies with lots of young users, that could potentially add up quickly, as the heads of the fictional video-chat company Pied Piper (from the popular HBO show "Silicon Valley") discovered when they faced the **possibility of $21 billion in COPPA penalties**.

If a parent, school, or anyone else has a complaint, concern, or question about COPPA, they can email the FTC at **CoppaHotLine@ftc.gov**.

Have any companies actually been sanctioned under COPPA?

Yes.

The most recent was in 2015, when two developers behind popular kids' apps such as My Cake Shop and Cat Basket agreed to pay $360,000 in civil penalties as part of a settlement with the FTC.

Large, well-known general-audience companies have been caught up in COPPA troubles, too. In 2014, Yelp agreed to pay a $450,000 civil penalty over a complaint that it had for years collected personal information from children without first getting parental consent.

And one of the larger COPPA settlements came in 2012, when the operator of fan websites for music stars such as Justin Bieber and Rihanna agreed to pay a $1 million civil penalty.

"Even a bad case of Bieber Fever doesn't excuse [operators'] legal obligation to get parental consent before collecting personal information from children," FTC Chairman Jon Leibowitz said at the time.

Additional Resources:

What is PPRA? Another student data privacy law

June 10, 2015

We hear a lot of conversation around FERPA and the need to update the law but there is another law that protects student privacy that has a different purpose, yet is no less important. That law is PPRA, the Protection of Pupil Rights Amendment. Both laws are important in that they provide protections for student privacy but they are different.

FERPA protects student educational records and ensures parental access to these records. It allows for a system enabling parents (or students) to correct inaccuracies in their records. FERPA also provides guidelines for who has access to these records and gives students the means to opt out of directory information (name, address, school clubs, etc.) that may be disclosed without consent unless a parent opts out of this disclosure.

But PPRA is completely different. PPRA's purpose is to allow parents to limit the kind of personal information that a school may collect from students. For example, this information can be collected as part of surveys, physical examinations, or certain evaluations. The law requires that schools obtain written consent from parents when students are required to participate in any U.S. Department of Education funded survey, analysis, or evaluation. A simple way to understand the difference between FERPA and PPRA is that FERPA protects information the school already has on record and PPRA protects information that schools do not have but can collect for surveys.

It is worthwhile to clarify that the law applies to U.S. Dept of Ed funded surveys. Not all surveys that come home are necessarily funded by the USDOE. However, in 2001 NCLB expanded PPRA to include all applicable surveys in public schools, not just those funded by U.S. Dept of Ed funds in 8 protected categories:

1. political affiliations or beliefs of the student or the student's parent;
2. mental or psychological problems of the student or the student's family;
3. sex behavior or attitudes;
4. illegal, anti-social, self-incriminating, or demeaning behavior;
5. critical appraisals of other individuals with whom respondents have close family relationships;
6. legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
7. religious practices, affiliations, or beliefs of the student or student's parent; or,
8. income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

In other words –

For surveys that contain questions from one or more of the eight protected areas that are not funded in whole or in part with Department funds, LEAs must notify a parent at least annually, at the beginning of the school year, of the specific or approximate date(s) of the survey and provide the parent with an opportunity to opt his or her child out of participating. LEAs must also notify parents that they have the right to review, upon request, any instructional materials used in connection with any survey that concerns one or more of the eight protected areas and those used as part of the educational curriculum.

So while PPRA doesn't cover all surveys it does cover surveys that collect information considered "intrusive". What I also learned is that it appears that in these cases, the surveysrequire prior parental consent otherwise the school cannot collect information from that student. And this is truly an opt-in option as opposed to an opt-out one. And worth noting that PPRA also has some other key requirements, besides surveys that have received little attention. Such as requiring that all instructional material (besides tests) be available to parents for review and (c)(1)(E) requires that every school have a local policy concerning "the collection, disclosure, or use of personal information collected from students for the purpose of marketing or for selling that information (or otherwise providing that information to others for that purpose), including arrangements to protect student privacy that are provided by the agency in the event of such collection, disclosure, or use."

While our first reaction is to opt out our children from any school survey we need to think about what we are opting out from. It is important to recognize that some of these surveys could provide valuable feedback to schools – are the right kids getting support, lunch assistance, or are our children being discriminated against because of their race or gender? These surveys could yield important information so that schools get adequate funding or professional assistance to address deficiencies that are identified. Of course, not all surveys' goal is to identify this. Others could be just aimed at marketing or addressing issues that we are not comfortable providing our children's information for. The process must be clear, the mechanism for opting out clear and easy in the event parents feel uncomfortable. Parents must know what the survey is for, who is conducting it, how it is funded, how their child's privacy will be protected. If we can trust the information we are given regarding the survey we can trust that if we decide to provide this information it will be used for the benefit of our children, and that is important.

I am a big advocate of having data and using it purposely. There is value in information. But parents must be given the information needed so that we can make informed decisions and be comfortable when providing details, sometimes extremely personal details, about our children.

Children's Internet Protection Act (CIPA)

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011.

What CIPA requires

Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them.

Schools and libraries must certify they are in compliance with CIPA before they can receive E-rate funding.

- CIPA does not apply to schools and libraries receiving discounts only for telecommunications service only;
- An authorized person may disable the blocking or filtering measure during use by an adult to enable access for bona fide research or other lawful purposes.
- CIPA does not require the tracking of Internet use by minors or adults.

You can find out more about CIPA or apply for E-rate funding by contacting the Universal Service Administrative Company's (USAC) Schools and Libraries Division (SLD) at sl.universalservice.org. SLD

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · www.fcc.gov/consumer-governmental-affairs-bureau

also operates a client service bureau to answer questions at 1-888-203-8100 or via email through the SLD website.

Filing a complaint

You have multiple options for filing a complaint with the FCC:

- File a complaint online at https://consumercomplaints.fcc.gov
- By phone: 1-888-CALL-FCC (1-888-225-5322); TTY: 1-888-TELL-FCC (1-888-835-5322); ASL: 1-844-432-2275
- By mail (please include your name, address, contact information and as much detail about your complaint as possible):

  Federal Communications Commission
  Consumer and Governmental Affairs Bureau
  Consumer Inquiries and Complaints Division
  445 12th Street, S.W.
  Washington, DC 20554

Alternate formats

To request this article in an alternate format - braille, large print, Word or text document or audio - write or call us at the address or phone number at the bottom of the page, or send an email to fcc504@fcc.gov.

Last Reviewed: 12/30/19