Privacy and Student Data: An Overview of Federal Laws Impacting Student Information Collected Through Networked Technologies

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

STUDENT PRIVACY INITIATIVE
Berkman Center for Internet & Society

PRIVACY AND STUDENT DATA:

An Overview of Federal Laws Impacting Student Information Collected Through Networked Technologies

June 2016

Dalia Topelson Ritvo

Berkman
The Berkman Center for Internet & Society at Harvard University

Youth and Media

23 Everett Street, 2nd Floor, Cambridge, MA 02138
www.cyber.law.harvard.edu/research/studentprivacy

ACKNOWLEDGEMENTS

Dalia Topelson Ritvo is the Assistant Director of Harvard Law School's Cyberlaw Clinic based at the Berkman Center for Internet & Society, and a Lecturer on Law at Harvard Law School.

This guide is based in large part on *Privacy and Children's Data: An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act*, which was published in by the Cyberlaw Clinic in November of 2013 as part of the Student Privacy Initiative. The Cyberlaw Clinic provides high-quality, pro-bono legal services to appropriate clients on issues relating to the Internet and technology, including privacy. 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 Student Privacy Initiative is a collaborative effort by the Berkman Center's Youth and Media Lab and the Cyberlaw Clinic to explore the opportunities and challenges that arise as educational institutions engage networked technologies both in and out of the classroom. This guide has been updated to reflect the work the Student Privacy Initiative has done to engage diverse stakeholder groups from government, education, academia, and business, among others, to develop shared practices that promote positive educational outcomes, while harnessing technological and pedagogical innovations without compromising student privacy and other critical values.

The Berkman Center is dedicated to the exploration, student, 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 challenges of cyberspace, particularly with regard to the need for normative and legal structures.

The Cyberlaw Clinic thanks its students, Makala Kaupalolo and Crystal Nwaneri for their help on preparing this publication. The Cyberlaw Clinic would also like to thank Paulina Haduong, Leah Plunkett, Sandra Cortesi and the Berkman Center's Executive Director, Urs Gasser, for their ongoing support of this publication.

INTRODUCTION

Over the past five years, schools have progressively been integrating the use of technology into the classroom, both to help students achieve their goals, and help teachers and administrators alike organize, categorize and track information about students. Specifically, "**Networked Services**" can be used in a variety of ways to improve school systems, including increasing efficiency in administrative operations to advancing individualized learning through online resources. Though these networked services may be valuable tools, they also have the ability to collect sensitive information about students. To that end, as educational institutions introduce networked services into schools, they must remain alert to growing privacy concerns for sensitive student information.

> Throughout this document, the term "**networked services**" is used to represent a range of services and devices that are connected through networked computers that educational institutions might employ. For example, cloud computing services are a type of networked service schools frequently use. "**Cloud computing**" refers to 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.
>
> Networked services also include the Internet of Things ("IoT"), which refers to the ability of devices to connect to the Internet and each other in order to collect and exchange data. These devices range from home temperature control systems to personal fitness trackers. In accordance with industry practice, laptops, smartphones, or tablets are not considered IoT devices in this document. Although these devices are commonly referred to as "smart" devices, the devices are in fact "dumb" without a website or application. These applications or websites may be considered networked services, but they would be more akin to a cloud computing service.

Harvard Law School's Cyberlaw Clinic, based at the Berkman Center for Internet & Society, has prepared this guide to provide a high-level overview of two of the major federal legal regimes that govern the privacy of children's and students' data in the United States: the Family Educational Rights and Privacy Act and the Children's Online Privacy Protection Act. In addition, this guide covers how the Protection of Pupil Rights Amendment, which, while not as broadly applicable to the use of technology by schools, does include a few provisions that can apply in certain contexts, particularly when schools use technology to administer surveys of student subjects, or use technology that collects information for marketing purposes. While there are other laws that may also apply to schools in this context (e.g. state privacy laws), these three laws have important implications for schools using networked services.

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 networked services to help educate students. All 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.

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 Secretary of Education ("DOE").[3] The institution may receive federal funding either (1) directly, through grants, cooperative agreements, contracts, subgrants, or subcontracts;[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 postsecondary 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] Examples of education records include personal contact information of students or parents, grades or test scores, disciplinary records, school health records, and similar information.[8] A "person acting for" the educational agency generally refers to agents of the school, such as teachers, administrators, and other school employees.[9] The Supreme Court has also stated that a person cannot be "acting for" an agency

unless he or she also "maintains" the record.[10] 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.[11]

What information is not considered an "education record"?

The following are not considered "education records" under FERPA:[12]

- 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;[13]
- records of an educational agency or institution's law enforcement unit;[14]
- records of employees of an educational agency or institution that are made during the normal course of business and relate exclusively to their employment;[15]
- records of students 18 years or older or attending a postsecondary school that are created by professionals, such as physicians or psychiatrists, for treatment purposes;[16]
- 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;[17] or
- grades on peer-graded papers before a teacher collects and records them.[18]

As schools engage more networked service providers, schools should consider how the use of these services might create additional education records. For example, if students are using online education tools, the records created using the product may be considered education records. Similarly, schools should consider whether data collected through IoT devices – for instance wearable fitness devices for physical education classes – would fall under the category of education record.

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.[19]

FERPA provides parents with four basic rights:

- the right to inspect and review educational records;[20]
- the right to challenge the content of education records and to correct or delete inaccurate, misleading, or inappropriate data;[21]

- the right to control the disclosure of education records containing their child's personally identifiable information via consent;[22] and

- the right to file a complaint regarding non-compliance of FERPA with the Department of Education (DOE).[23]

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.[24] Personally identifiable information includes:[25]

Certain educational technologies will rely on information protected by FERPA. For example, if a school uses online learning systems that require creating individual student accounts, the school might give the provider information from education records, including names and contact information. Privacy Technical Assistance Center, Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices (2014).

- 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.[26]

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.[27]

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;[28]
- to seek amendment of records;[29]
- to consent to disclose personally identifiable information;[30] and
- to file complaints with the DOE if the educational institution violates these provisions.[31]

The annual notice must also include the procedures eligible students must follow to review and amend documents.[32] 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.[33]

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.[34] 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.[35]

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;[36]
- the parties' "legitimate interests" in requesting or obtaining such information;[37] 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.[38]

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, so 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.[39] 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.[40] Directory information does *not* include: social security numbers, student ID numbers.[41]

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.[42]

De-identified data may include metadata, which is contextual or transactional data that networked services providers collect as part of their operations.[43] Metadata may include useful information such as how many attempts a student made at a task before successful completion.[44] Once any direct and indirect identifiers have been removed from the metadata, it is not considered personally identifiable information under FERPA.

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. The 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.[45]

Schools may disclose ***personally identifiable information*** without prior parental consent to the following parties and in the following circumstances:[46]

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. In addition, if designated a school official, cloud computing service providers are limited by FERPA in what they can do with this information. Providers may not repurpose information – they may only use it for the original purpose for which it was shared.

- to school officials with "legitimate educational interests," including the "educational interests of the child for whom the consent would otherwise be required;"[47]
- to a contractor, consultant, or volunteer or another entity to which the institution has outsourced " 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;[48]
- to officials of another school where a student is transferring;[49]
- to specified officials for audit or evaluation purposes;[50]
- to determine financial aid for a student;[51]
- to organizations conducting certain studies for or on behalf of the school;[52]
- to comply with a judicial order or lawfully issued subpoena, perpetration of a crime, or disciplinary proceeding;[53]
- to appropriate officials in cases of emergency to protect the health and safety of the student or other individuals;[54]
- to state and local authorities, within a juvenile justice system, pursuant to specific state law;[55] or
- to accrediting organizations.[56]

Additional resources to learn 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
- https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf
- http://ptac.ed.gov/
- http://ptac.ed.gov/sites/default/files/cloud-computing.pdf

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Overview

The Children's Online Privacy Protection Act[57] and the Children's Online Privacy Protection Rule[58] (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.

Who does COPPA apply to?

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.[59]

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:[60]

- 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."[61] 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."[62] A "corporation" is defined as an entity that "is organized to carry on business for its own profit or that of its members."[63] 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.[64]

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.[65] 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.

Even if a school is not subject to FTC oversight, schools may engage cloud computing service providers or use IoT connected devices from companies that are likely to be subject to the FTC's jurisdiction. To that end, any time a school engages a cloud computing service provider or employs a new technology for use, 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.[66] 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 expressly 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 minimum, operators are

expected to maintain the confidentiality of information collected from parents when they provide consents for the release of their child's information or when they review information collected from their child.[67]

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. [68] 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.[69]

> Active data collection in the networked services context could refer to email providers or online resources that solicit personal information from students.
>
> Passive data collection may be especially relevant to IoT devices that rely on sensors to consistently track a user's behavior. For example, with the growing popularity of wearable fitness trackers, schools may implement these devices in physical education classes. While in use, the devices are continuously tracking and recording data about its user, in this case, a student.

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.[70]

   The content of the parental notice must include all of the content that COPPA requires an operator to disclose in his privacy policy. Additionally, it must state:[71]

   - 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.[72]

2. **Obtain 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.[73] 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 he or she collects such information:[74]

- solely to provide direct notice and obtain parental consent;
- to respond to a child's specific request on a one-time basis;[75]
- to send the child periodic communications, including online newsletters, site updates, or password reminders;[76]
- 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.[77]

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.[78] 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.[79]
- 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.[80]

Can a school consent on behalf of parents?

Schools may consent on parents' behalf when the collection, use, or disclosure of personal information from students is ***conducted solely for the school's benefit.***[81] This means that a school may consent on behalf of parents, so long as the operator only uses the information on behalf of the school pursuant to the agreement between the school and the operator.[82] 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.[83]

How can an operator obtain consent from schools?

When obtaining consent from educational institutions, operators must comply with all notices required under COPPA, and must provide to the school "full notice of its collection, use, and disclosure practices."[84] Upon the school's request, an operator must furnish a description of the personal data collected, give the school an opportunity to review and delete the personal information, and prevent any additional collection or use of the personal information.[85] Further, in order for the consent to be valid, the operator must employ "***reasonably calculated***" methods to ensure consent is obtained from the school and not children.[86]

In addition to the consent requirements, the FTC recommends that school districts or schools, not individual teachers, should predetermine which operators have appropriate information practices before using a service.[87] Schools should also make operator's notices about the information practices available to parents.[88] Schools – or schools districts – may wish to notify parents of all the operators who have been approved for use.

3. Disclosure 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.[89] 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.[90]

However, an operator *may* 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.[91]

If a website operator wants to share a child's personal information with an affiliate for *any other reason,* the operator must notify parents of its intention to do so both in its direct notice to parents and in its privacy policy. The direct notice must state whether the affiliate will be bound by the operator's privacy policy and give parents the chance to opt out of the such a disclosure.[92]

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:[93]

- 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;

The content of the privacy policy must also state:[94]

- 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.[95] General audience websites must contain a link to the privacy policy on the homepage of the children's area of its website.[96] The FTC suggests using a larger font size, different color, or a contrasting background for emphasis.[97]

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.[98] 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.[99] If approved, the operator is offered a "safe harbor" from complying with COPPA's requirements so long as the operator complies with the self-regulatory program approved by the FTC.[100] For information about applying for FTC approval of a safe harbor program, see C.F.R. Section 312.11, business.ftc.gov/privacy-and-security/children's-privacy, or email CoppaHotLine@ftc.gov.[101]

Additional resources to learn about COPPA

- https://www.law.cornell.edu/uscode/text/15/chapter-91
- http://www.ftc.gov/ogc/coppa1.htm
- http://www.ftc.gov/os/fedreg/2013/01/130117coppa.pdf
- https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools
- 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

PROTECTION OF PUPIL RIGHTS AMENDMENT

Overview

The Protection of Pupil Rights Amendment (PPRA)[102] was originally enacted in 1978, granting parents of minors and eligible students certain rights regarding surveys, analyses, or evaluations administered through any program funded by the DOE.[103] Specifically, the original statute allows parents and eligible students to both: (1) inspect any materials "used in connection with any survey, analysis, or evaluation" as part of any program funded by the DOE,[104] and (2) opt out of any survey, analysis or evaluation that involves any of the following information:

- political affiliations or beliefs of the student or the student's parent;
- mental or psychological problems of the student or the student's family;
- sex behavior or attitude;
- illegal, anti-social, self-incriminating, or demeaning behavior;
- critical appraisals of other individuals with whom respondents have close family relationships;
- legally recognized privileged or analogous relationships (e.g. lawyers, doctors and clergy);
- religious practices, affiliations, or beliefs of the student or student's parent; or
- income.[105]

In 2001, the PPRA was expanded as part of the No Child Left Behind Act.[106] This amendment imposes additional obligations on K-12 institutions to implement certain policies regarding surveys conducted on students. Specifically, K-12 institutions must notify parents and eligible students of certain activities, and allow parents and eligible students to opt out of certain activities. Most relevant with respect to networked services, the PPRA imposes obligations on activities that involve collecting, disclosing, or using students' personal information for marketing or sales purposes. Rights granted under PPRA transfer to the student once the student is 18 years old or is an emancipated minor.[107]

Who does the PPRA apply to?

Generally, the PPRA applies to the "programs and activities of [a State Education Agency, Local Education Agency], or other recipient of funds under any program funded by the U.S. Department of Education."[108] The portion of PPRA that was added as part of No Child Left

Behind (subsection (c) of the statute) is limited to Local Education Agencies (LEAs), which the statute defines as "an elementary school, secondary school, school district, or local board of education … but does not include a postsecondary institution."[109]

What additional obligations does PPRA impose on LEAs?

1. Develop policies:

LEAs must work with parents to develop policies regarding:[110]

- Parents' right to request and inspect any third party survey before it is administered or distributed to students, including arrangements to protect student privacy if the survey concerns the type of information described in the PPRA overview above.[111]

Schools may choose to administer a survey of their student body using a third-party survey tool or platform. If these surveys examine any of the protected categories of information, schools must ensure that the platform is sufficiently secure to protect the information collected through the platform.

- Parents' right to request and inspect "any instructional material used as part of the educational curriculum for students," as well as procedures for granting such a request;

- Students' personal information that is collected, disclosed, or used for the purpose of marketing or selling the information, except when such personal information is collected for the "exclusive purpose of developing, evaluating, or providing educational products or services"[112] for students or schools, including the following circumstances:[113]

    - college or military recruitment;

    - programs providing access to low-cost literary products, including book clubs and magazines;

    - curriculum and instructional materials;

    - tests and assessments used to "provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information about students," and the "subsequent analysis and public release of the aggregate data from such tests and assessments;"

    - students' sales of products or services to raise funds for school-related activities; and

- programs for student recognition.

- The administration of physical examinations or screenings that the LEA may administer to a student;

- Parents' right to request and inspect any instrument used in obtaining information that is collected, disclosed, or used for the purpose of marketing or selling the information, as well as procedures for granting such a request.

2. Notify parents and eligible students of policies

LEAs must, at a minimum, directly notify parents of the policies described above on an annual basis at the beginning of the school year and within a reasonable time period after any substantive policy changes are made.[114] In addition, LEAs must notify parents when any specific activities are scheduled or expected to be scheduled, and should include approximate dates.[115] Specifically, LEAs must notify parents of any of the following events:

- Any survey involving the protected categories of information;

- Any activities that involve collecting, disclosing, or using students' personal information "for the purpose of marketing or for selling that information (or otherwise providing that information to others for that purpose)."[116]

- Any nonemergency, invasive physical examination or screening that is administered and required by the school, and not necessary to protect the immediate health and safety of the students.

3. Provide parents and eligible students the opportunity to opt-out of certain activities

In addition to the general requirement under the PPRA to allow parents and eligible students to opt-out of any surveys involving the eight categories of sensitive information defined in the statute, LEAs must offer parents an opportunity to opt-out from having their child participate in any activity involving the collection, disclosure or use of students' personal information for the purpose of marketing or selling the information "(or otherwise providing that information to others for that purpose)."[117]

At first glance, PPRA may not seem to relate to schools' use of networked services. However, because PPRA concerns arise when personal information is collected directly from students, there may be instances where students using online education tools may divulge information that implicates PPRA. For example, PPRA requires LEAs to notify and allow parents to opt-out of any activities that involve collecting, disclosing, or using students' personal information for marketing or sales purposes. If LEAs are contracting with cloud computing providers for services that may lead to the marketing or sale of student information, then the school must give parents the opportunity to opt-out from having their children participate in the activity. For instance, PPRA would prohibit a school from using an email service provider that uses a student's personal information to provide targeted ads to that student, unless proper notification and opportunity for opt-out were provided.

Additional resources to learn about PPRA

- https://www.law.cornell.edu/uscode/text/20/1232h
- https://www.law.cornell.edu/cfr/text/34/98.1
- http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html
- http://www2.ed.gov/policy/gen/guid/fpco/hottopics/ht04-10-02.html
- http://familypolicy.ed.gov/ppra?src=fpco
- https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf

DEFINITIONS

FERPA

Personally Identifiable Information (PII): Includes a student's name, a family member's name, address, personal identifiers (e.g. social security number, student number), indirect identifiers (e.g. date of birth or place of birth), and other information that a "reasonable person in the school community" could use to identify the student.

Education Records: Materials maintained by an educational agency or "by a person acting for such an agency or institution," and "contain information directly related to a student."

Directory Information: Information including a "name, address, telephone listing, date and place of birth, major field of study, weight and height . . . dates of attendance, degrees and awards received" most recently attended school, and participation in sports or activities. Excludes social security numbers.

De-Identified Data: Data is de-identified when the school has removed all PII and there is "a reasonable determination that a student's identity is not personally identifiable."

PPRA

Personal information: Individually identifiable information, including a student or parent's name, home address, telephone number or a Social Security number.

Instructional material: Instructional content provided to a student, including "printed or representational materials, audio-visual materials, and materials in electronic or digital formats." Excludes academic tests or assessments.

Invasive physical examination: Any medical examination involving the "exposure of private body parts, or any act during such examination that includes incision, insertion, or injection into the body." Excludes a hearing, vision, or scoliosis screening.

Local educational agency (LEA): An elementary or secondary school, school district, or local board of education that receives funds from an applicable program. Excludes postsecondary institutions.

COPPA

Personal Information: Includes a first and last name, home address, email address, telephone number, or social security number, a persistent identifier "used to recognize a user over time and across different Web sites," photo, video, audio files containing a child's voice or image, geo-location information, and "any other information that permits physical or online contact of a specific individual."

Disclosure: With regard to personal information, the release of identifiable personal information from a child, with the exception of providing the information to someone for internal support of the website. Making personal information publicly available and identifiable through a website's home page, pen pal service, email service, message board, or chat room.

FERPA:
- 20 U.S.C. § 1232g
- 34 C.F.R. § 99

COPPA:
- 15 U.S.C. § 6501

PPRA
- 20 U.S.C. § 1232h

[1] The Family Educational Rights and Privacy Act (FERPA), Pub. L. No. 93-380 (1974), codified at 20 U.S.C. § 1232g. The
[2] 20 U.S.C. § 1232g (2012); see also Gonzaga Univ. v. Doe, 536 U.S. 273, 276 (2002).
[3] 34 C.F.R § 99.1(a) (2016); 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 Jun. 8, 2016).
[4] 34 C.F.R § 99.1(c)(1) (2016).
[5] Id. § 99.1(c)(2).
[6] Id. § 99.1.
[7] 20 U.S.C. § 1232g(a)(4)(A) (2012).
[8] Questions and Answers about Education Records, U.S. DEP'T OF EDU., https://www2.ed.gov/about/overview/focus/daca-education-records.pdf (last visited Jun. 8, 2016).
[9] See Owasso Independent School District v. Falvo, 534 U.S. 426, 433 (2002).
[10] Id. at 433–34.
[11] Id.
[12] 34 C.F.R. § 99.3("Education records")(b)(1) (2016); see also FERPA Frequently Asked Questions (FAQ), PA. STATE UNIV., http://www.registrar.psu.edu/confidentiality/FERPA_faq.cfm (last visited Jun. 8, 2016) [hereinafter PSU FAQs].
[13] 34 C.F.R. § 99.3("Education records")(b)(1) (2016).
[14] Id. § 99.3("Education records")(b)(2).
[15] Id. § 99.3("Education records")(b)(3).
[16] Id. § 99.3("Education records")(b)(4).
[17] Id. § 99.3("Education records")(b)(5).
[18] Id. § 99.3("Education records")(b)(6).
[19] See 20 U.S.C. § 1232g(d) ("[W]henever 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 Jun. 8, 2016) [hereinafter FERPA FAQs].
[20] 20 U.S.C. § 1232g(a)(1)(A) (2012).
[21] Id. § 1232g(a)(1)(D)(2).
[22] Id. § 1232g(b)(2); 34 C.F.R. § 99.30(a) (2016).
[23] 34 C.F.R. §§ 99.7(a)(2)(iv), 99.63 and 99.64 (2016).
[24] Id. §§ 99.30(a) and 99.31.
[25] Id. § 99.3 ("Personally Identifiable Information").
[26] Id. § 99.30(b).
[27] Id. § 99.30(d).
[28] Id. § 99.7(a)(2)(i).
[29] Id. § 99.7(a)(2)(ii).
[30] Id. § 99.7(a)(2)(iii).
[31] Id. § 99.7(a)(1)(iv).
[32] Id. § 99.7(a)(3)(i)–(ii).
[33] Id. § 99.7(b).
[34] Id. § 99.32(a)(1).
[35] Id. § 99.32(d).
[36] Id. § 99.32(b)(1)(i)–(ii).
[37] Id. § 99.32(b)(1)(i)–(ii).
[38] Id. § 99.32(a)(1).
[39] 20 U.S.C. § 1232g(a)(5)(B) (2012).
[40] FERPA FAQs, supra note 18.
[41] 34 C.F.R § 99.3 ("Directory information")(b)(1)–(2) (2016).
[42] Id. § 99.31(16)(b)(1).
[43] Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices, PRIVACY TECHNICAL ASSISTANCE CENTER., https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf (last visited Jun. 8, 2016)
[44] Id.
[45] Id. § 99.31(16)(b)(2).
[46] Id. § 99.31(a).
[47] Id. § 99.31(a)(1)(i)(A); 20 U.S.C. § 1232g(b)(1)(A) (2012).
[48] 34 C.F.R. § 99.31(a)(1)(i)(B) (2016).

[49] Id. § 99.31(a)(2); id. § 99.34(a).
[50] Id. § 99.31(a)(3)
[51] Id. § 99.31(a)(4).
[52] Id. § 99.31(a)(6)(i).
[53] Id. § 99.31(13)–(16).
[54] Id. § 99.36(a).
[55] 20 U.S.C. § 1232g(a)(5)(E) (2012).
[56] Id. at § 1232g(a)(5)(G).
[57] 15 U.S.C. §§ 6501–6506 (1998).
[58] 16 C.F.R. § 312 (2013).
[59] 15 U.S.C. § 6501(2) (1998); 16 C.F.R. § 312.2 (2013).
[60] See 16 C.F.R. § 312.2 (2013) (definition of "Website or online service directed to children").
[61] 16 C.F.R. § 312.2 ("Operator") (2013).
[62] 15 U.S.C. § 45 (2012).
[63] Id. at § 44.
[64] 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) (1998) (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].
[65] 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 (2012).
[66] 16 C.F.R. § 312.2 ("Personal information") (2013).
[67] 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.").
[68] 16 C.F.R. § 312.2 (2013).
[69] 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).
[70] 16 C.F.R. § 312.4 (2016).
[71] Id.
[72] Id.
[73] Id. § 312.5(a).
[74] 16 C.F.R. § 312.5(c) (2016).
[75] Id. § 312.5(c)(3); see also 78 Fed. Reg. 3972, 3993 (Jan. 17, 2013).
[76] 16 C.F.R. § 312.5(c)(4) (2016); see also 78 Fed. Reg. 3972, 3993 (Jan. 17, 2013).
[77] Id. § 312.5(c)(5).
[78] 16 C.F.R. § 312.5(b) (2016). See also COPPA FAQs, supra note 61, Questions C(11) and C(12).
[79] Id.
[80] Id.
[81] Id.
[82] COPPA FAQs, supra note 61, Questions M(1)–M(3).
[83] Id.
[84] Id.
[85] Id.
[86] Id.
[87] Id.
[88] COPPA FAQs, supra note 61, Questions M(4).
[89] 16 C.F.R. 312.8 (2016).
[90] Id.; See also COPPA FAQs, supra note 61, Questions M(2)–M(3).
[91] COPPA FAQs, supra note 61, Questions I(6)–I(10).
[92] Id.
[93] 16 C.F.R. § 312.4(d) (2016).
[94] Id.
[95] Id.
[96] Id.
[97] COPPA FAQs, supra note 61, Question C(8).
[98] 16 C.F.R. § 312.10 (2016).
[99] Id. § 312.11.

[100] Id. § 312.11(g).
[101] COPPA FAQs, supra note 61, Questions N(1)–N(3).
[102] PPRA is also known as the Hatch Amendment, Grassley Amendment, or Tiahart Amendment. Hot Topics: Recent Changes Affecting FERPA and PPRA, U.S. DEPARTMENT OF EDUCATION (Apr. 7, 2006), http://www2.ed.gov/policy/gen/guid/fpco/hottopics/ht04-10-02.html. The Protection of Pupil Rights Act (PPRA) is codified at 20 U.S.C. § 1232h. The regulations that administer PPRA are found in 34 C.F.R. § 98.
[103] PPRA for Parents, U.S. DEPARTMENT OF EDUCATION (Apr. 7, 2006), http://www2.ed.gov/policy/gen/guid/fpco/ppra/parents.html.
[104] 20 U.S.C. § 1232h(a) (2012).
[105] Id. at § 1232h(b).
[106] Supra note 101.
[107] 20 U.S.C. § 1232h(c)(5)(b) (2012).
[108] See FERPA Frequently Asked Questions, FAMILY POLICY COMPLIANCE OFFICE, http://familypolicy.ed.gov/faq-page/14#t14n251 (last visited Jun. 8, 2016).
[109] 20 U.S.C. § 1232h(c)(6)(C) (2012).
[110] U.S. DEPARTMENT OF EDUCATION, supra note 1.
[111] 20 U.S.C. § 1232h(c)(1)(b) (2012).
[112] Id. at § 1232h(c)(4)(A).
[113] Id. at § 1232h(c)(4)(A).
[114] Id. at § 1232h(c)(2)(A).
[115] U.S. DEPARTMENT OF EDUCATION, supra note 1.
[116] 20 U.S.C. § 1232h(c)(2)(C)(i) (2012).
[117] Id. at § 1232h(c)(2)(C)(i).