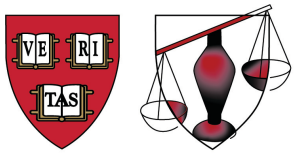

Research Publication No. 2013-23
November 2013

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).