Student Privacy Boot Camp for EdTech Companies

COPPA and FERPA

March 3, 2016

Emily S. Tabatabai

NOTHING IN THIS PRESENTATION IS INTENDED TO CONSTITUTE A LEGAL OPINION

Children's Online Privacy Protection Act

COPPA

ORRICK

Children's Online Privacy Protection Act

- What is COPPA?
  - Children's Online Privacy Protection Act - Federal law enacted in 1998
  - Law directed the Federal Trade Commission (FTC) to create and enforce rules relating to the online privacy of children's information. The FTC's Children's Online Privacy Protection Rule was effective in 2000 and amended in 2012.
- Enforcement and penalties
  - Violations can carry penalties up to $16,000 per violation.
  - Penalties also include data destruction, 20 year reporting requirements
  - FTC enforces aggressively (25 public consent decrees since 1999)
    - Penalties range from $35,000-$3,000,000
  - State Attorneys General may also enforce the Rule

Who is Covered?

The Rule applies to operators of commercial websites and online services (including mobile apps) that collect, use or disclose personal information from children under 13 in the following instances:

1. The website or online services is **directed to** children under 13, or
2. The general audience website or service has **actual knowledge** that it is collecting information from children under 13.

"Directed To"	"General Audience Site"
Subject matter Visual content Use of animated characters Child-oriented activities Music or audio content Age of models Child celebrities Language Advertising directed to kids Intended audience	Collect birth date Notified by child or parent also , Knowledge that operator is collecting info from kids on a site that is directed to kids (i.e. plug-ins, ad networks)

ORRICK

What is Personal Data?

"Personal Information" of children under 13 is defined very broadly to include:

- First and last name
- home address including street name and name of city
- online contact information (email address, user name, screen name)
- telephone number
- social security number
- persistent identifier (ex. cookie) that can be used to recognize the user over time
- photograph, video or audio file that contains the child's image or voice
- geolocation information sufficient to identify street name and name of city
- information collected by third party whose content or plugin is collecting information on the Operator's site
- any other information about the child or the child's parents that the operator combines with the identifiers described above

What is Required?

- Post a clear and comprehensive **online privacy policy**
- Provide **direct notice to parents** and **obtain verifiable parental** consent before collecting PI online from children
- Give parents **the choice** of consenting to the operator's collection and use of a child's PI, but prohibiting the operator from disclosing that PI to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents)
- Provide parents **access** to their child's PI to review and/or have the information deleted
- Give parents the opportunity to deny or rescind consent to use child's PI
- **Maintain the confidentiality, security, and integrity of information** they collect from children, and
- **Retain** PI collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and **delete** the information using reasonable measures to protect against its unauthorized access or use.

What Can I Collect Without Parental Consent?

•Must obtain parental consent before collecting personal information from the child, unless the collection fits into one of the limited exceptions to prior parental consent

•Exceptions to prior parental consent

- For purpose of obtaining consent - When sole purpose of collection is to provide notice to parent and obtain parental consent. May collect name, email address and email address of parent. If consent is not obtained, must delete the information.
- One time contact - When operator collects online contact information and no other information, for the sole purpose of responding one time to the child; PI is not used for any other purpose or to re-contact the child; PI is deleted after one-time contact
- Internal Operations - When operator collects a persistent identifier and no other information and it is used solely to provide support for internal operations of the website

How Can I Get Parental Consent?

Operator must obtain parental consent through a means "reasonably calculated," in light of available technology, to ensure that the person providing consent is the child's parent.

Email Plus

If operator uses information only for internal purposes and will not share the information with third parties, you may use "Email Plus"

1. Send email notice to parent that provides information on the collection and use of child's information (Rule sets forth what must be included in notice)
2. Receive parental consent (usually via reply email)
3. Follow up with confirmation email, fax, or telephone call to parent. Include parental notice information again, along with instructions on how to opt-out.

Verifiable Parental Consent

If operator uses information to share with third parties or to share publicly (or facilitate a means by which the child can share publicly), you must obtain verifiable parental consent. Methods:

- consent form to be signed by parent and returned by mail, fax, or electronic scan
- credit or online payment transaction ($$)
- taking phone calls through toll-free telephone number or engaging in video conference
- checking form of government-issued ID
- knowledge-based identification
- consent mechanism provided by Safe Harbor provider

How Can I Avoid The Hassle and Expense?

Most companies go to great lengths to avoid collecting information from children that would trigger COPPA parental consent requirements.

- Do not collect personal information
- Collect only persistent identifiers that will be used solely to support internal operations
- Implement an **Age Screen** to screen out kids under 13. If you have a general audience site (i.e., the site is not directed to kids under 13), you can block kids under 13 from providing personal information by implementing an Age Screen

Neutral Age Screen

Age screen mechanism must be age-neutral and not encourage falsification

Mechanism should request user to enter age accurately (i.e., require user to freely enter day, month, and year)

Do not warn the kid that users under 13 will not be permitted to participate

Use non-specific language when user is blocked ("Sorry, you are not permitted to register at this time)

Use cookie to prevent back-buttoning to try again

COPPA and Schools

If an operator is offering an online program solely for the benefit of students and the school, the school can act as the parent's agent and can consent to the collection of kids' information on the parent's behalf

- School can consent to the collection of children's information solely for educational purposes, and no other commercial purpose
  - i.e., operator cannot use children's data for other purpose, like marketing, advertising, sharing with other parties unrelated to the educational context. If Operator wants to use student data for other commercial purpose, must get parental consent
- Operator must provide school with COPPA notices, and provide (on request) a description of PI collected, an opportunity to review/delete the child's PI, and opt-out of further collection
- Prefer consent to come from the school or district, rather than teacher. School should have contract with Operator
- Must delete children's PI once information is no longer needed for educational purpose
- Best practice: School should provide parents with notice of operators who collect and use children's information (Acceptable Use Policies for Internet Use)
- Examples of Operators who may presume consent from Schools: homework help lines, education modules, research tools, web-based testing services

COPPA Safe Harbor Programs

- Rule created “Safe Harbor” program whereby an Operator is deemed to be in compliance with COPPA if it adheres to a set of self-regulatory guidelines approved by the FTC. To be approved by the FTC, the guidelines must be at least as restrictive as COPPA.
- Most are merely self-regulatory compliance programs, which are overseen and audited by the organization. PRIVO, Imperium (ChildGuard Online), and Aristotle (Integrity System) have parental consent tools as well.
- TRUSTe consent decree (November 2014) found that TRUSTe did not adequately maintain its oversight function and misled consumers as to the strength of its program.

Approved Safe Harbor Programs (as of 12/2015)

- CARU
- ESRB
- Privo
- TRUSTe
- Aristotle International, Inc. (“Integrity”)
- kidSafe
- Imperium (“ChildGuard Online”)
- iKeepSafe

Resources

- Read the Rule
  http://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16:1.0.1.3.36&rgn=div5
- Read the FAQs (last revised March 20, 2015)
  http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions#General Questions
- FTC 6-Step Compliance Plan for Your Business
  http://www.business.ftc.gov/documents/bus84-childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business
- Browse the FTC website section on children's privacy

Family Educational Rights and Privacy Act

FERPA

Family Educational Rights and Privacy Act

What is FERPA?

- Federal law that applies to educational institutions that accept public funds
- Prohibits a school from disclosing **personally identifiable information** from a **student's educational record** to a third party without **consent** from the parent. There are several exceptions, however.
- Provides parents the right to inspect and correct the information contained in the student record
- Rights transfer to the student when the student turns 18 or enters Higher Ed at any age.

Enforcement

- FERPA is enforced by the Department of Education. School is responsible for (and liable for) compliance of its vendors and service providers.
- Issue a complaint, cease and desist order, withhold further funding from Dept.
- Seeks voluntary compliance before imposing sanctions

What Type of Data Does FERPA Protect?

"Educational Records" – Records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the educational agency or institution

"Personal Information" – direct identifiers (such as a student's or family member's name) and indirect identifiers (such as date of birth, mother's maiden name)

- Exceptions:
  - De-identified Data – De-identified data is data which has been stripped of all direct identifiers as well as indirect identifiers that may in combination identify a particular individual, may be shared with third parties without consent
  - Metadata – Metadata is contextual or transactional data (ex. data about how long a student took for a particular activity, when the activity was completed, etc.) that has been stripped of all direct and indirect identifiers is not covered by FERPA
  - (These data points *could* still be Personal Information if a reasonable person in the community could identify the individual student with this data in combination with readily available public information).

When is consent not required for disclosure?

An educational agency or institution may disclose personally identifiable information from the educational record without consent in limited circumstances, including:

- To a School Official with a legitimate educational interest
- To federal or state educational authority in connection with audit and evaluation of federally supported education program
- To a representative of the Attorney General for law enforcement purposes
- In connection with a student's application for financial aid
- Person designated in a federal grand jury subpoena or other subpoena
- Accrediting organizations carrying out accrediting functions
- Organizations conducting studies for purposes of developing, validating, administering predictive tests, administering student aid programs, improving instruction
- Directory information not subject to these disclosure limitations, as long as student can opt-out

Directory Information

- "Directory Information" – information contained in the educational record that would not generally be harmful if disclosed, including student name and address.
- Usually, directory information includes name, telephone number, date and place of birth, honors and awards, clubs and sports, dates of attendance
- School should establish which elements are considered "directory information" and notify parents that this information may be shared publicly. Parents usually have the right to **opt-out** of the sharing of directory information

→ Because parents have the ability to opt-out of Directory Information disclosures, this makes it difficult for EdTech providers to rely on Directory Information to supply necessary student data

To Be a "School Official"

Schools usually share data with a vendor/provider under the "School Official" exception to FERPA. Under this exception, Schools may share PII from the educational record without parent consent as long as the provider:

- Performs a service or function for which the school would otherwise use its own employees (i.e., acts as a outsourced service provider)
- Is under the **direct control** of the school with regard to the collection and use of data
- Uses data only for authorized purposes and does **not re-disclose** PII from educational record to other parties unless with consent of School or permitted by FERPA
  - **TIP:** These restrictions (i.e., Direct Control; authorized use; and prohibition against re-disclosure) should be established in the contract between the school and the provider. Sometimes, these can be established in the online Terms of Service (TOS)
    - See slide on "Tip: Elements to Include in a Contract" at end of presentation

Obligations of EdTech vendors

- Remember, when Personal Information is disclosed to the EdTech vendor, FERPA still governs its use! And the School is in control of, and responsible for, its protection.
- EdTech vendor must:
  - Request only the personal information required for a particular task
  - Not use personal information for purposes other than those disclosed in the contract with the school
  - Not disclose student data to a third party without direction from and consent of school
  - Maintain appropriate physical, technical and administrative safeguards to protect student personal information
  - Create and maintain comprehensive security incident response policy and plan to notify in the event of a breach
  - Destroy personal information at the end of the contract term

FERPA Resources

FERPA Regulations, https://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf

Final Regulations, with comments, published by Department of Education, http://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf

Privacy Technical Assistance Center:

- Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices, https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf
- Responsibilities of Third Party Service Providers Under FERPA, http://ptac.ed.gov/sites/default/files/Vendor%20FAQ.pdf
- Model Terms of Service, http://ptac.ed.gov/sites/default/files/TOS_Guidance_Jan%202015_0.pdf

Other Rules that May Apply

•**Protection of Pupil Rights Amendment (PPRA)** – (among other things) requires school to provide notice and opt-out rights to parents if students are going to participate in an activity involving the collection, disclosure, or use of PI collected from students and that will be used for marketing purposes (applies only to K-12 institutions)

•**European Data Protection Directive** – Generally, the same EU data protection law applies to student data as well, and may be more restrictive

- Breaking News: US-EU Safe Harbor deemed invalid on Oct 6, 2015
- Awaiting details on US-EU Privacy Shield

TIP: Elements to Include in Contract

To qualify to receive student records under the "School Official" exception, the service provider should agree to certain contractual provisions. Provisions also required under State Laws.

•Establish that the School "owns" the data and vendor will use it only according to terms of the contract and for the purpose to benefit the School

•What data elements will be collected or received from the School

•How data will be used by the vendor (explicit use)

•Restrictions against ability to share/re-disclose data to third parties, unless specifically consented to in the agreement

•Restrictions against using data for marketing, including behavioral targeting, or profile-building

•Caveat that vendor may use de-identified data, metadata or data that is shared under "directory information" exception for its own purposes, including to share with third parties

•Data retention and destruction policy

•Data security provisions, including each party's responsibilities in the event of a data breach

TIP: Many Schools are under-staffed and lack legal counsel, and School representatives look to the Service Provider to confirm compliance with FERPA, COPPA and state laws

Emily S. Tabatabai

Emily S. Tabatabai is a founding member of Orrick's Cybersecurity and Data Privacy team, which is nationally ranked by the *Legal 500 US.* As a Certified Information Privacy Professional in both European and US law (CIPP/EU, CIPP/US), she counsels companies on all matters of data privacy and consumer protection law, with a special focus on retail products, EdTech, online dating and social media, mobile and online gaming, and all manner of entrepreneurial start-up endeavors. Emily works with clients to evaluate compliance with multi-national laws, regulations, and best practices, and represents companies subject to regulatory investigations or litigation involving a spectrum of federal and state laws.

etabatabai@orrick.com

blogs.orrick.com/TrustAnchor

@EmilyTabatabai

ORRICK

ORRICK

Trust Anchor

An established point of trust in a cryptographic system from which a process of validation can begin

Blog: blogs.orrick.com/trustanchor
Twitter: @Trust_Anchor