COPPA 101

Amelia Vance, Future of Privacy Forum

Linnette Attai, PlayWell LLC

Sara Kloek, SIIA

Emily S. Tabatabai, Orrick Herrington & Sutcliffe

November 2017

Children's Online Privacy Protection Act (COPPA): The Fundamentals

Linnette Attai
PlayWell, LLC

About PlayWell, LLC

- Full-service compliance consulting
- Virtual Chief Privacy Officer & Data Protection Officer
    - Serving industry, nonprofit organizations, schools and districts
- Backed by 25 years of compliance experience
- Technology assessments, policy and process development, training, crisis communications
    - GDPR, FERPA, COPPA, PPRA, state student data privacy laws, marketing regulation, compliant innovation

Children's Online Privacy Protection Act

- What is COPPA?
  - Federal Trade Commission
    - Parental control
    - Data minimization
    - Transparency
    - Reasonable security

Compliance Requirements

- Compliance requirements:
  - Obtain verifiable parental consent before collecting, using or disclosing personal information collected from a child under the age of 13
  - Allow parents to review child's data/request that it be deleted or prevent further collection of data
  - Minimize data collection
  - Ensure that third parties can and do comply
  - Post a prominently displayed, accurate privacy policy

COPPA Basics

- Who must comply?
  - Directed in whole or in part to children
  - Actual knowledge
  - Children as a primary or secondary audience
  - General audience site or service with children's section
- Do you need to comply?
  - Totality of circumstances test

Personal Information Under COPPA

- First and last name
- Home, school or other physical address
- Online contact information
- Screen or user names that function as online contact information
- Phone number
- Social Security number
- Geolocation (street and city/town)
- Photographs, videos and audio files
- Persistent identifier used to recognize a user over time and across sites or services
- Other data collected about a child or child’s parent when combined with any of the above

Persistent Identifiers

- When is a persistent identifier not considered to be personal information?
  - Internal operations
- Third party due diligence

Notice and Verifiable Parental Consent

- Notice requirements
- Methods for notice
  - One time use exception
  - Multiple contact exception
  - Deletion of data prior to posting

Parent Rights

- Consent/withdraw consent
- Review
- Stop contact
- Collect but don’t disclose
- Delete data

COPPA & Schools

Sara Kloek
SIIA

“I think all would agree that proficiency with the Internet is a critical and vital skill that will be necessary for academic achievement in the next century. The benefits of the Internet are
extraordinary.”

- Senator Richard Bryan (D-NV) introducing COPPA on July 17, 1998

COPPA's 1999 Final Rule

"…the Commission notes that the **Rule does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parents' agent in the process**. For example, many schools already seek parental consent for in-school Internet access at the beginning of the school year. Thus, where an operator is authorized by a school to collect personal information from children, after providing notice to the school of the operator's collection, use, and disclosure practices**, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent**…"

COPPA’s 1999 Final Rule

“To ensure effective implementation of the Rule, the Commission also intends to provide guidance to the educational community regarding the Rule’s privacy protections.”

COPPA FAQ M.1

1. Can an educational institution consent to a website or app's collection, use or disclosure of personal information from students?

Yes. Many school districts contract with third-party website operators to offer online programs solely for the benefit of their students and for the school system – for example, homework help lines, individualized education modules, online research and organizational tools, or web-based testing services. **In these cases, the schools may act as the parent's agent and can consent to the collection of kids' information on the parent's behalf**….

COPPA FAQ M.2

2. Under what circumstances can an operator of a website or online service rely upon an educational institution to provide consent?

Where a school has contracted with an operator to collect personal information from students for the use and benefit of the school, and for no other commercial purpose, **the operator is not required to obtain consent directly from parents, and can presume that the school's authorization for the collection of students' personal information is based upon the school having obtained the parents' consent.**

COPPA FAQ M.3, M.4, M.5

- M.3 recommends best practices on who at the school may provide consent.
- M.4 recommends that, as a best practice, schools should consider providing parents notice of technology for which it has consented.
- M.5 outlines what sorts of information a school should seek out from an operator prior to providing consent.

So how does COPPA actually work in the schools?

¯_(ツ)_/¯

FERPA's School Official Exception & COPPA's School Consent Process

FERPA

1. Performs an institutional service or function for which the school or district would otherwise use its own employees;
2. Has been determined to meet the criteria set forth in in the school's or district's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records;
3. Is under the direct control of the school or district with regard to the use and maintenance of education records; and
4. 4. Uses education records only for authorized purposes and may not re-disclose PII from education records to other parties (unless the provider has specific authorization from the school or district to do so and it is otherwise permitted by FERPA).

COPPA

A school's ability to consent for the parent is limited to the educational context – where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose.

COPPA Enforcement & Compliance

How companies get into trouble

Emily S. Tabatabai
Orrick Herrington & Sutcliffe

Enforcement and penalties

- FTC Enforcement
  - Penalties up to $40,000 per violation (up from $16,000)
  - Consent decrees can also include data destruction; 20 year reporting requirements
  - Enforced aggressively (30 public consent decrees since 1999)
  - Penalties range from $35,000-$4,000,000
  - (Fines sometimes partially suspended due to inability to pay)

- State Attorneys General may also enforce the Act

How do they find you?

- Data Breach
- Industry Sweep
- Targeted Enforcement
- Consumer Complaints

Enforcement Themes

Directed to Children

Ignorance of the law is no excuse

LAI Systems (2015) – Developer of kid-directed apps (My Cake Shop, My Pizza Shop) did not ask for kids' PI but permitted online advertising from 3rd parties	$60,000
RetroDreamer (2015) – Same facts, different apps (Happy Pudding Jump, Ice Cream Drop)	$300,000
TinyCo (2014) - Online kid-directed gaming apps (Tiny Pets, Tiny Zoo, Tiny Village and Mermaid Resort) did not ask for consent.	$300,000
Skidekids.com (2011) – Website dubbed the "Facebook and MySpace for kids" allowed kids to post video and messages without consent	$100,000

Enforcement Themes

Actual Knowledge

But it's not a kids site!

InMobi (2016) – mobile ad network failed to honor developer check-box that provided notice that app was "child directed"	$4,000,000
Yelp (2014) – Asked for voluntary birthdate, but mobile app did not include age screen	$450,000
RockYou (2012) – Developer of widgets for social network sites asked for birthdate without age screen; data breach of legacy system exposed 32M user accounts	$250,000

Enforcement Themes

Insufficient COPPA notice/consent

Didn't get it quite right….

United Artists Arena (2012) – Operator of music fan websites collected birthdates: (i) didn't ask for parent email address for Email+ notice; (ii) or send insufficient notice	$1,000,000
Playdom (2011) – child-directed and general audience sites had age screen, but insufficient notice and no verifiable consent before permitting kids to post publicly	$3,000,000
Xanga (2006) – social network age screen said, "*You hereby certify to Xanga that you are at least 13 years old. Xanga is intended for people who are at least 13 years old. Children under 13 are not permitted to join Xanga or participate in the Xanga Community.*"	$1,000,000

NY AG: "Operation Child Tracker"

NY AG settlement with Hasbro, Viacom, Matel, and Jumpstart (2016)

1. **Operator liable for downstream activities of 3rd parties on site**
   - Ad trackers "piggybacking" on analytics cookies
   - 3rd party embedded content (YouTube and 3rd party plug-ins)
2. **Mixed-use site must comply with COPPA even if children aren't primary audience**
   - Mixed use site (even if kids are small portion of audience) must assume all visitors are children and implement age screen
   - No OBA on mixed-use site without age screen
3. **Strict liability for mistakes**
   - Inadvertent tracker placement, Coding errors

Viacom ($500,000), **Matel** ($250,000), **Jumpstart** ($85,000), **Hasbro** ($0)

Lessons Learned

1. Don’t ask for birthdate without an age screen!
2. If you get consent, be sure to do it correctly
3. Take affirmative steps to monitor and oversee the third parties operating on site: *Can you scan for rogue trackers? Contractually limit piggy-backing? Extremely challenging due to complexity of ad ecosystem!*
4. Carefully consider your audience: *is it directed to children at least in part? Is it directed to adjacent age group?*
   - *Be careful of login pages!*
5. Employee training: *does your digital marketing team understand COPPA?*
6. Check, check, check: *mistakes can be costly*

Wait…no enforcement?

- Images
- Audio
- Internet of Things / Devices
- EdTech

Emily S. Tabatabai

Emily is a founding member of Orrick's Cybersecurity & Data Privacy practice, which was named Privacy Practice Group of the Year by Law360 in 2016, and praised in Legal 500 USA for offering a team with "very specific industry knowledge and extremely appropriate advice."

Emily advises companies on a wide range of data privacy laws and cutting-edge data-use cases – including student data privacy and child-directed services, biometrics, geolocation, retail tracking, robotics and connected devices, digital advertising, and Big Data. The Legal500 specifically highlights Emily's expertise and "extraordinary depth of knowledge in student data privacy matters," which includes her representation of leading innovators in the Ed-Tech space.

She lives with her family in Texas, and yes, people rarely mess with her.

Emily S. Tabatabai
Of Counsel, Orrick Herrington & Sutcliffe
Cybersecurity & Data Privacy Practice

202-339-8698
etabatabai@orrick.com
http://blogs.orrick.com/trustanchor/
Twitter @EmilyTabatabai

COPPA Resources

- Read the Rule
  https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf
- Read the FAQs (last revised March 20, 2015)
  https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools
- 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
  https://www.ftc.gov/consumer-protection/childrens-privacy