COPPA 101 Webinar Meeting Notes

(open to all education privacy working groups and Student Privacy Pledge signatories)

Friday, November 10, 2017
1:00pm-2:00pm
Topic: COPPA 101 Webinar
64 Attendees

Contents

<u>Linnette Attai, Compliance Consultant, at PlayWell, LLC on Children's Online Privacy Protection Act: The Fundamentals</u>

Linnette@PlayWell-LLC.com, 917-485-0353

Children's Online Privacy Protection Act (COPPA)

- COPPA is a law enforced by the Federal Trade Commission.
- The purpose is to allow parents to have control over what their kids are allowed to access online, specifically if the child is under the age of 13

Compliance Requirements

- Obtain verifiable parental consent
- Allow for parental controls
- Must allow for the deletion of data
- Have reasonable security
- Ensure that third party partners also have reasonable security standards
- Must have a prominent, accurate privacy policy on the website (think contrasting colors and a decent font size)

Who Must Comply?

- Persons with actual knowledge that children are the primary or secondary audience of their online services
- The website is directed in whole or in part to children (perhaps the site has animations, children activities, ads directed to children, visuals for children, etc)
- If you have a mixed use website, you should treat all persons on the website as though they are under the age of 13 unless you implement an age gate/screen

What is protected under COPPA?

- Information that can be used to identify or contact a child:
    - Phone numbers
    - First and last name
    - Home, school, or other physical address
    - Social Security Number, etc
- A persistent identifier is not considered to be personal information when it's used for internal operation.

Verifiable Parental Consent

- You must obtain verifiable parental consent before collecting information from a child. Notice must be sent to the parent letting them know what information you plan to use, how you plan to use the information, and you must include a link to the privacy policy.
- There are a variety of methods approved by the FTC to provide notice and gain parental consent:
    - a credit card or online payment (the most common),
    - a signed form which can be sent back via email or fax,
    - check against a government issued ID,
    - email plus, etc.
- There are very few exceptions to this rule. Those are below:
    - One time use exception, for example: a "contact us" form, you must delete after responding
    - Multiple Contact Exception
    - Deletion of data prior to posting

Parent Rights

- Parents have the right to review data collected from their child
- Approve the collection but not disclose of information collected from their child
- Request for Data to be deleted
- Ask that contact be discontinued

Sara Kloek, Director of Education Policy at SIIA, Presentation on COPPA & Schools

- COPPA's Introduction in the Senate:
    - After COPPA was passed, FTC released the final rule in 1999.
- FERPA still plays a large role in how schools treat student data and COPPA's School Consent Allowance
- The Protection of Pupil Rights Amendments is also relevant:
    - Governs the administration to students of a survey in protected areas
    - Also concerns marketing surveys
    - Does NOT apply to the collection disclosure, or use of personal information collected from students, etc
- COPPA remains largely unclear, but the FTC does have a list of frequently asked questions on their website under Section M.

M. COPPA AND SCHOOLS

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. However, the 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. Whether the website or app can rely on the school to provide consent is addressed in FAQ M.2. FAQ M.5 provides examples of other "commercial purposes." ...

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. However, the operator must provide the school with full notice of its collection, use, and disclosure practices, so that the school may make an informed decision....

3. Who should provide consent – an individual teacher, the school administration, or the school district?

- As a best practice, we recommend that schools or school districts decide whether a particular site's or service's information practices are appropriate, rather than delegating that decision to the teacher. Many schools have a process for assessing sites' and services' practices so that this task does not fall on individual teachers' shoulders.

4. When the school gives consent, what are the school's obligations regarding notifying the parent?

- As a best practice, the school should consider providing parents with a notice of the websites and online services whose collection it has consented to on behalf of the parent. Schools can identify, for example, sites and services that have been approved for use district-wide or for the particular school...

5. What information should a school seek from an operator before entering into an arrangement that permits the collection, use, or disclosure of personal information from students?

- In deciding whether to use online technologies with students, a school should be careful to understand how an operator will collect, use, and disclose personal information from its students. Among the questions that a school should ask potential operators are:
  - What types of personal information will the operator collect from students?
  - How does the operator use this personal information?
  - Does the operator use or share the information for commercial purposes not related to the provision of the online services requested by the school? For instance, does it use the students' personal information in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the online service? If so, the school cannot consent on behalf of the parent.
  - Does the operator enable the school to review and have deleted the personal information collected from their students? If not, the school cannot consent on behalf of the parent.
  - What measures does the operator take to protect the security, confidentiality, and integrity of the personal information that it collects?
  - What are the operator's data retention and deletion policies for children's personal information?

For more information, please see Section M at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools

Emily S. Tabatabai, Orrick Herrington & Sutcliffe, COPPA Enforcement & Compliance
etabatabai@orrick.com, 202-339-8698

Enforcement and Penalties

FTC Enforcement:

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

State Attorney Generals may also enforce COPPA

How do you become the target of an FTC investigation?

- There is a data breach, and sometimes this causes the FTC to investigate your company
- Industry Sweep
- Targeted Enforcement, this happens with the FTC wants to make a particular point about certain privacy concerns
- Consumer Complaints, this happens when consumers, possibly parents complain about the website

Enforcement Themes

- Your product is Directed to Children, and in this case, ignorance of the law is no excuse, and it doesn't matter how big or small your company is
- Your product is not directed to children but you have actual knowledge that children are using your website; i.e. this happens when there is an age screen, and children are still allowed to use the website
- Your website provides insufficient COPPA notice/consent
- Example: New York AG "Operation Child Tracker"
    - Operator liable for downstream activities of 3rd parties on website
        - Ad trackers "piggybacking" on analytic cookies
    - Mixed-use site must comply with COPPA even if children aren't primary audience
        - No OBA on mixed-use site without age screen
        - Mixed use site (even if kids are small portion of audience) must assume all visitors are children and implement age screen
    - Strict liability for mistakes
        - Inadvertent tracker placement, coding errors

Lessons Learned

- Don't ask for a birth date without an age screen
- If you get consent, be sure to do it correctly
- 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!
- Carefully consider your audience: is it directed to children at least in part? Is it direct to adjacent age groups?

- Employee training: Does your digital marketing team understand COPPA? Make sure they understand how their ad partner's technology works.
- Check for mistakes
- Adopt vetting procedures for third parties: determine when and how they'd decided whether to permit other use of the data on their site
- Consistently scan your site for issues

Question & Answer

Could Linnette explain more about what it means to remove PI from user generated content before posting when she was talking about exceptions (or perhaps give an example)?

> Answer: For example, when you ask a student to take pictures of flowers, but they do so with their phone, then they send it to you, it also includes location data. This location data should be removed. Also, remove children's information from chatrooms, where sometimes, the children over disclosure. Remove any PII before posting.

The FTC recommends the following, "If, however, an operator intends to use or disclose children's personal information for its own commercial purposes in addition to the provision of services to the school, it will need to obtain parental consent. Operators may not use the personal information collected from children based on a school's consent for another commercial purpose because the scope of the school's authority to act on behalf of the parent is limited to the school context." How does a vendor navigate getting consent? How do they know when a school provides consent but can only give "limited consent" for educational purpose?

> Answer: The school can only provide consent for educational purposes under COPPA. They cannot do this for targeting advertising for that is a use that a school simply cannot consent to. Also, although the operator under COPPA may obtain consent to use this data for other purposes, there are a variety of other laws that should be considered when thinking about using student data for commercial purposes. How consent is dealt with should also be addressed in the contract.

How does COPPA apply to web extensions, as with Google extensions and app plugins? Example: Parents have consented to Google for Education (or district has worked with Google to designate Google Ed suite as "school official" under FERPA). Yet, third party extensions are available that change the feature set of these apps, and also can collect PII. Typically, we don't block these (as we could for other websites under CIPA) because doing so would also block Google (already approved).

> Answer: Extension should be thought of as ads. If they are collecting personal information from children then you must get consent. You must figure out who is responsible for that third party collection. The answer to that question may depend on how that extension is provided and what it's collecting.

Can a teacher consent on the behalf of a school if the tools we provide are picked up by individual teachers, instead of the entire school?

Answer: The FTC only offers "best practice" guidance on this and suggests schools come up with policies to outline a proper consent process. FERPA should also be considered in this situation. - Sara Kloek, SIIA

Teacher consent may violate FERPA - either the school/district is allowing teachers to bind the district via contracts (or Terms of Service, in this case), or the teacher is putting student information into an app without authorization from the school/district, which violates FERPA. Even if the school/district allows teachers to consent on their behalf, if the Terms of Service the teacher is agreeing to does not comply with FERPA (see USED's great model terms of service guidance for help on this), than it violates FERPA - Amelia Vance, FPF

A good practice is to ensure that your terms of use specify that the person agreeing must be authorized to bind their organization. - Linnette Attai, PlayWell, LLC

How do operators know when school provide consent because they are required to only use student information for school purposes? How does the operator know which users need to be gated from other commercial users?

Answer: Many companies working in the school market will sign contracts that outlines consent, as well as a data maintenance and deletion process. - Sara Kloek, SIIA

A "click wrap" agreement, in combination with the privacy policy, should also include all the information that Sara laid out above. The operator determines whether or not they need to age-screen users based on the "totality of circumstances" test that I described to determine whether or not it is directed to children. If children are a secondary audience, age screening is needed. If you do not believe children under 13 are using your site or service, but you gain actual knowledge that they are (for example, you learn that it's being used in a 4th grade class), you will need to reassess your compliance with COPPA. As a bit of general guidance, if your product is designed to be used in schools, be careful about how you use the personal information such that it is only used for the school purpose. Also remember that for products not used in schools, any commercial uses of data often means disclosure, which requires prior parental consent. And of course, state student data privacy laws often prohibit use of student data for targeted advertising and make no exception for it to be permitted with parental consent- Linnette Attai, PlayWell, LLC

What about chat features? We collect verifiable parental consent for the entire product but the product has a chat feature. What if children share PII through those features and we do not plan on assigning trained staff to filter all PII e.g., children coding their PII or breaking down PII such that filters cannot catch everything? (We will ensure there are reasonable filters i.e., censor certain words, etc.) Do we need consent to have this feature or just provide notice in the privacy policy that chat features exists and that children may share PII? I know that if we do assign such trained staff, then this could mean actual knowledge.

Answer: Yes - you will need to obtain prior parental consent for the chat feature if you do not plan to delete any personal information that children may share before posting their chat. In

addition, allowing children to share PII in a chat feature can present very real safety risks, so consider not just COPPA, but also physical safety risks that may result. This - more often than any privacy issue - is an area where I see significant missteps. - Linnette Attai, PlayWell, LLC

What about video services like FlipGrid that records children's faces, voices, unique identifier and other? When a teacher ads their entire class, how does the teacher ensure that the images and recordings will only be used for school services? How do teachers identify what services have the capacity to separate children's PII collected from schools verses children's PII collected with parental consent?

Answer: COPPA's FAQ M.5 outlines some questions to ask when evaluating technology to be used in the classroom. Also, the Department of Education's Model Terms of Service has a great resource for evaluating terms of service: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Mar2016.pdf.

How will vendors manage state specific requirements for accountability like Colorado that can have parents request a "hearing" to address privacy issues.

Answer: There are a variety of ways that vendors are working to get into compliance with the state student data privacy laws. Those hearings will most likely be run in conjunction with the school/district, not between the parent and vendor. Happy to discuss the specifics further offline. - Linnette Attai, PlayWell, LLC

How do vendors manage the unique identifier COPPA compliance requirements when school owned devices are assigned to one child for both school and personal use of an 8-year old. This unique device is always connected to young child sites. When this specific child goes to additional sites, owned by commercial vendors for entertainment and not approved by the school official, what is required.

Answer: Not sure I fully understand the question. Are you asking as a device provider or as an operator of a site or service being used on the device? The operator of a site that now has use and knowledge of the unique identifier connected with the child/student.

If you have actual knowledge that the device is used by children, and the device is used in grade school, then you may need to adjust accordingly. Happy to discuss and get more information to give you a more tailored answer. - Linnette Attai, PlayWell, LLC

If we don't ask for age (e.g. how old are you?), but ask the child for his/her grade (e.g. what grade are you in?), is that considered PII?

Answer: Grade, when not combined with any other information, would not be considered PI under COPPA. However, grade is not a clear indicator of age, and so can't necessarily be used to

age screen. - Linnette Attai, PlayWell, LLC

Can companies require schools to "comply" with COPPA for them by say that they are in charge of collecting parent signatures?

Answer: The FTC only has Section 5 authority over operators. - Sara Kloek, SIIA

An operator may not designate a school as an "operator." Just as an operator can not "comply" with FERPA, only align with it, operate in support of the school's compliance, etc., a school can't really "comply" with COPPA. They can, however, obtain the consent, and the operator may rely on the school having obtained the consent when there is a contract in place. - Linnette Attai, PlayWell, LLC

We have private schools that claim they are exempt from these federal laws. I'd like to make 100% sure that's okay. Some of them have partnerships with public schools, so in that case, I assume they would not be exempt, correct?

Answer: FERPA applies to schools receiving money from the U.S. Department of Education which typically includes public schools. There are some cases where a private school would need to follow FERPA but these cases are not common.
COPPA does not apply to schools. It applies to commercial operators. Commercial operators would need to meet COPPA's notification and consent requirements when they are collecting information from children under the age of 13.
Regarding partnerships with public schools, this is likely a very case by case situation. Happy to talk more about this offline. - Sara Kloek, SIIA

In addition, keep in mind that state student data privacy laws generally do not distinguish between public and private institutions, and most of the state laws reiterate many of the requirements of FERPA. - Linnette Attai, PlayWell, LLC

What happens when a school becomes the provider of the site or service? Like we use a module that is open source, but it's our learning management system. Are we then required to be COPPA compliant? I assume yes, but …

Answer: The school is never an operator under COPPA. COPPA only applies to the operator of the site or service. - Linnette Attai, PlayWell, LLC

Is there a practical reason that I'm missing as to why non-profits are exempt from COPPA? My experience has been that tools built by universities, for example, are among the most objectionable in terms of what student data privacy info they provide and how they intend to use and retain data.

Answer: Yes, the FTC does not have the authority to regulate nonprofits. So, they recommend that nonprofits comply, but can't compel them to do so. Some emerging federal student data

privacy legislation attempts to extend FTC's purview, but we'll see if there's tolerance for that. - Linnette Attai, PlayWell, LLC

How do social media plug-ins (e.g. Twitter "like" button) work in terms of data collection? Do websites targeted to kids always have to avoid using these?

Answer: They are all actually a bit different, and there is a combination of factors that needs to be considered, including whether or not we are dealing with a link or plug in, what data is transmitted and whether or not the social media platform age screens its users. In addition, some social media platforms have "child directed" configurations so that their plug-in can be embedded on a child-directed site or service if configured properly. Happy to discuss further offline. - Linnette Attai, PlayWell, LLC

Examples (from FPF):

- Facebook Social Plugins: https://developers.facebook.com/docs/plugins/
- Facebook for Child-Directed Sites: https://developers.facebook.com/docs/plugins/restrictions
- "This document includes the alternative code that you are required to use for our Social Plugins and the Facebook SDK for JavaScript in the United States and any other country or state where applicable laws require child-directed sites and services to distinguish themselves from other general audience sites, apps or services."

How do YouTube embedded videos work in terms of their data collection? Do we always need to avoid embedding these videos into a child-directed site?

Answer: Generally, yes, the YouTube player can not be embedded on child-directed sites. The YouTube embedded video player includes social media plug ins that passively transmit data, and YouTube itself is not actually intended for children. YouTube passively collects persistent identifiers for ad-serving purposes. - Linnette Attai, PlayWell, LLC

Can de-identified student data be used to track which "types of kids" respond respond best to specific marketing campaigns without violating COPPA? Can you have groups at all under COPPA? Or is that not allowed because you are creating a profile by assigning characteristics to various kids to say they are part of a group?

Answer: You can run standard analytics on child-directed sites and services. So the answer to your question is dependent on what you mean by "types of kids." Generally ad effectiveness can be measured, but extreme care must be taken when implementing to ensure that you and your third parties are not profiling for ad-serving purposes, and are not using the information for behavioral targeting (and other targeting, if you take state student data privacy laws into consideration). - Linnette Attai, PlayWell, LLC

Exactly how much point-in-time advertising-related "analytics" is covered by the "internal operations" exception of COPPA? Example: an advertiser can serve ads to kids, even contextual

ads, but how much can that advertiser measure (1) who, or how many people (%), saw &/or clicked the ad, (2) conversion (e.g. know that x% of people who saw the ad downloaded a different app by the same developer - this can be done by using mobile "vendor ID" which allows identifying the same mobile user but only to the developer - not useful across the broader web), (3) measurement of attribution or "brand lift" (measure that x% of people who saw the ad went the brand's website or the physical store)

Answer: These are very specific questions that are probably best discussed offline, but I'll ty to provide some general parameters: First, there is no exception under COPPA for measuring ad effectiveness. Thus, it is not necessarily about "how much" but rather "what information" is used to measure ad effectiveness and how. Second, remember that if you are tracking across unrelated sites and services, this gets into a complex area that may not be acceptable under COPPA. It is very much dependent on what is being done and how. There are also other laws that may be triggered here. Please feel free to contact me to discuss in more detail - Linnette Attai, PlayWell, LLC

Do security and retention requirements still apply even if data is collected through the "internal ops" exception?

Answer: Security and retention requirements generally apply to the personal information. So if you are collecting personal information and not disclosing it, the security and retention requirements apply. If you are collecting a persistent identifier only for internal operations, you have more leeway, unless you end up connecting that persistent identifier with other PI, in which case, you have to treat it as it is PI.. - Linnette Attai, PlayWell, LLC

Just to make sure I understand - if you do not publish non-de-identified data on students under 13, then you can use the email plus method to get verifiable consent? And using things like Google Analytics still counts under "internal operations," right?

Answer: If you publish personal information about students under the age of 13, email plus may not be used. Email plus may only be used when the information is not published. However, if we're dealing with a school use situation, the school may provide consent in lieu of the parent if the information is used for the school purpose and no other commercial purpose. And yes, things like Google Analytics are considered "internal operations," however be sure it is configured properly and that the ad-tracking features are turned off on your dashboard. - Linnette Attai, PlayWell, LLC

I am not aware of any k-12 schools receiving a fine or penalty because of FERPA violation. Are Universities the primary target for FERPA enforcement from the Dept of Education?

Answer: FERPA's main enforcement action is remediation, which unfortunately the public rarely hears about - when a school violates FERPA and the violation is reported to the Dept of Ed, Ed determines whether the school has actually violated FERPA and, if so, they work with the school to fix it. FERPA does allow Dept of Ed to take away all federal funding if a school violates

FERPA, but REQUIRES that there be an opportunity for remediation before that happens. It has never happened (as you can imagine, schools usually fix whatever it is pretty quickly when Dept of Ed knocks at their door).

Actions are taken against universities more frequently for privacy violations, but not because of FERPA - universities are also subject to GLBA and their contract agreements to access the Dept of Ed's financial aid database. If they have security issues that violate either of those, the Dept of Ed can cut off their access to the database, and they may be subject to GLBA penalties as well. - Amelia Vance, FPF

Has an state attorney general enforced any new state privacy laws? Not COPPA but laws such as SOPIPA? With all the new state laws, what are the trends with enforcement?

Answer: Not yet. We're waiting… (Emily Tabatabai)

My bet is we'll likely see an action first from California, Colorado, or Connecticut. However, all of these laws are still very new - even though California's law was passed in 2014, it didn't go into effect until 2016, and there are many definitions in the law that could lead to misunderstandings that the AG's office may choose to resolve through working with the vendor instead of an action against them. Hard to know. - Amelia Vance, FPF.

What k12 privacy laws provide parents the Right of Action? Federal? State?

Answer: It has been a while since I looked at this, so apologies if my information is out-of-date. As of 2014, Alabama (Code of Ala. § 31-13-27), Idaho (Idaho Code § 33-133), Illinois (105 ILCS 10), New Hampshire (RSA 193-E:5), Ohio (ORC Ann. § 1347.10.), Rhode Island (R.I. Gen. Laws § 16-38-5.1), and Virginia (Va. Code Ann. § 2.2-3800-3809) allowed for a private right of action (not always directly by parents, though - ex/ Idaho's has to be a civil enforcement action brought by the state board of ed). Several state laws explicitly ban a parent private right of action for student privacy violations, instead relying on parental complaints to the state education agency or state AG office - Amelia Vance, FPF

What about state auditors? For the states like MO, that have a state auditor holding districts accountable for data governance with the same high standards as other public institution, have any enforcement consequences followed the schools with poor audit results?

Answer: I believe that the main tool used by the Missouri State Auditor was public shaming, and it worked: there were a ton of news articles, and when she checked back in with the districts she had audited this year, massive improvements had been made. - Amelia Vance, FPF

(Coincidentally, I was in Missouri yesterday speaking with districts about student data privacy. A book of policies just dropped from MSBA with governance recommendations for schools in Missouri as well. Not sure if other states will follow suit. - Linnette Attai, PlayWell, LLC)

Has the FTC enforced any student privacy requirements on a vendor? If the schools are not a commercial entity, does the FTC have the capacity to enforce student privacy laws? What about a private school? Can the FTC enforce student privacy laws if the school is not a public school?

Answer: With the exception of FERPA, most of the student privacy laws have been passed by the states and many apply directly to the vendor (as opposed to FERPA which applies only to the school). In other words, states can enforce these laws against the vendor instead of focusing enforcement on the school. The FTC is not able to enforce compliance with state laws, but the FTC could bring a deceptive practices case if an operator makes deceptive statements regarding its privacy practices. (Emily Tabatabai)

The FTC recommends, "Schools also should ensure operators to delete children's personal information once the information is no longer needed for its educational purpose." How does a vendor know when a school no longer needs the vendor to retain a child's PII?

Answer: That is a great question that often causes confusion, particularly as school contracts often renew annually over time. The data retention / deletion practices should be addressed in the vendor/school contract. The vendor could rely on the school to determine if a student's data is "no longer needed," in which case the school could request deletion or could control the deletion of student data manually. You should also consider dormancy - if a user account has been dormant for some time, it could have long passed the point at which it is no longer necessary to maintain, even if the school did not direct the vendor to delete that data specifically. (Emily Tabatabai)

Also be sure to consult with the state laws, many of which have defined data retention periods, some requiring deletion when the contract terminates. However, as Emily notes, be sure you are defining a retention period in your agreement, or outlining a policy in your terms if you don't use a written contract. For contracts that renew annually, you can accrue a good deal of risk in the event of a security incident by holding onto the data for many years when it's not necessary to have it on hand to operate the product for the school. - Linnette Attai, PlayWell, LLC

Is there any guidance as to how this applies in a Smart TV context, which might collect viewing information tied to a persistent identifier?

Answer: There's not very specific guidance, but examining your privacy practices to ensure they are consistent with applicable law and that you are not operating in a manner that gives you actual knowledge that you are collecting viewing information tied to a persistent identifier and are using it in a way that would trigger a COPPA compliance requirement. (Also, consider your VPAA compliance. Several companies have been targeted around that over the past few years, although so far those attempts at litigation have not been successful.) - Linnette Attai, PlayWell, LLC

FTC states, "However, the 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." What mechanism needs to built by vendors to manage these children with only limited permission?

Answer: If you plan to use data collected from students for other commercial purposes, you will need to obtain verifiable parental consent through one of the processes mentioned in the webinar. Be sure to consult with state student data privacy laws as well, as some of them restrict use of student data for commercial purposes, and parents can't consent to that use. - Linnette Attai, PlayWell, LLC

What can school do to make the process of limited consent easier for vendors? What can be done with click through agreements?

Answer: I'm not sure schools really have a role to play in making the consent process easier for vendors. As it is, the vendor need only rely on the contract with a school to indicate that the school will be managing the consent process. In addition, a click-wrap is a contract. (The FTC has said, "a contract is a contract"). The vendor does, however, need to ensure that they are providing the school with "full notice of its collection, use, and disclosure practices, so that the school may make an informed decision." (COPPA FAQ M2) - Linnette Attai, PlayWell, LLC

Who consents for a student when a child uses a device provided by the teacher through a Go Fund Me campaign? The device is not owned by the school or by the parent? Can a individual teacher consent on their own personal devices?

Answer: Not sure I understand - is this a situation where the teacher has given a child his or her personal device for a funding campaign? - Linnette Attai

The questions on this list focus on COPPA, however, the FTC also enforces HIPAA. In the school setting, some schools contract with mental health professionals to work with students. The school contracts directly with the health care provider. (This is not a separate clinic connected to school.) When behavioral health and mental health services are offered through a school contracted provider, how can confidentiality be maintained when FERPA parent rights conflict with student's mental health confidentiality in states like CA?

Answer: As a starting point, there is some good HIPAA/FERPA joint guidance available here: full notice of its collection, use, and disclosure practices, so that the school may make an informed decision. In terms of conflicts between CA state law and FERPA in this specific area, it would be helpful to line the laws up after first assessing whether or not the mental health information is part of the education record covered by FERPA. - Linnette Attai, PlayWell, LLC

Is the student's first initial plus last name considered PII (no other personal information is collected).

Answer: It depends on how unique the name is.

Does PPRA allow marketing surveys as long as there has been notice and parental consent? Is it always clear what constitutes a marketing survey in the Ed Tech context?

Answer: PPRA is concerned with administering surveys, analyses or evaluation that require students to provide certain sensitive information. Although some areas of PPRA permit certain marketing for limited items (for example, for colleges, military recruitment, book clubs, curriculum materials), it doesn't "allow marketing surveys." In addition, keep in mind that the permissive areas of PPRA around marketing may conflict with marketing restrictions in state student data privacy laws. - Linnette Attai, PlayWell, LLC

Resources

1. Read the Rule: https://www.ftc.gov/system/files/documents/federal_register_notices/2013/01/2012-31341.pdf
2. Read the FAQs (last revised March 20, 2015) https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools
3. 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
4. Browse the FTC website section on children's privacy https://www.ftc.gov/consumer-protection/childrens-privacy
5. CoSN Protecting Privacy Toolkit http://cosn.org/privacy