Ad Tech & Ed Tech Call 2: Legal Frameworks

Wednesday, July 27, 2017
Time: 3:00pm-4:30pm

Table of Contents

Sara Kloek (U.S. Department of Education) on Advertisements and FERPA

USED Regulatory Frameworks

- USED oversees two separate privacy laws: FERPA and PPRA
- There is a fine line between personalized learning, content recommendations, and advertising.
- USED does not currently have specific guidance on advertising technology but the department does have guidance on educational technology. (linked in the google doc and available at studentprivacy.ed.gov)

FERPA

- The Family Educational Rights and Privacy Act (FERPA) is the primary student data privacy law.
    - FERPA puts requirements on public k-12 schools and most public and privacy higher education institutions to protect the privacy of student education records.
    - Gives parents and eligible students (18+ or enrolled in post-secondary education) access to student records for viewing and correction.
- Schools are using educational technology services which may need access to education records to perform these services.
- There are a couple of ways schools can disclose student information for these services or other purposes.
    - Students can consent to disclose information in student education records with some basic specificity as to what information will be disclosed and to whom.
    - Schools may disclose student information without consent through the school official exception in FERPA.
    - The school official exception requires:
        - The service provider must perform a service that would normally be the responsibility of the school;
        - The service provider must meet the "school official criteria" set out in the school's annual FERPA notice;
        - The student information shared by the school must remain in the direct control of the school; and
        - The company may only use the education record for authorized purposes and may not re-disclose PII from the educational record.
    - Additionally, some information (Directory) information may be disclosed without consent.
    - Some services do not use student PII and thus are not subject to FERPA.

FERPA and Advertising

- USED generally does not consider advertising to be a legitimate educational purpose under FERPA's school official exception.
- USED does not allow advertising to be included as an educational purpose for vendor/school contract terms.

Protection of Pupil Rights Act

- The PPRA applies solely to K-12 students and gives parents certain rights when information is collected from children.
    - Including for marketing purposes.
    - There is a large amount of exceptions that cannot be covered within the scope of this call.
    - For more information, please studentprivacy.ed.gov

<u>Question:</u> What enforcement actions the department can take a provider discloses student PII in an impermissible way?

Answer: FERPA applies directly to schools. If a school violates FERPA and the school refuses to come into compliance the department may withhold federal funds from the school. If a school shares information with a service provider and that service provider mistreats the data the department may ban the school from using that ed tech provider for a minimum of five years.

***Question:** What are some of the steps that both ed tech companies and schools should take to manage their responsibilities around advertising technologies?*

Answer: The U.S. Department of Education provides some great guidance on best practices for using online services and ed tech. The model terms of service also goes through some clauses to avoid when reviewing terms of service. Schools and ed tech vendors can also contact the U.S. Department of Education with any questions or concerns.

Lydia Parnes (Wilson Sonsini Goodrich & Rosati) on COPPA & FTC Enforcement

COPPA Overview

- COPPA (1998) was enacted long after FERPA and has been amended twice since its enactment.
- The primary goal of COPPA is to place parents in control over what information is collected from their children online.
- The COPPA rule is the primary vehicle for the FTC to enforce the act.
- The FTC frequently puts out guidance for companies to comply with various COPPA rules. This came in the form of 50 or so FAQs which are updated on a pretty regular basis. (available here)
- COPPA applies to any website, app, or any online service that is directed in full or in part to children under 13 or where the online service has actual knowledge that is collecting personal information from kids under 13.

COPPA Requirements and Application

- There are three main requirements of the COPPA rule.
    - A service provider must give parents notice and obtain their consent before collecting, using, or disclosing personal information from kids under 13.
    - The online service must honor a parent's request to access or delete information that is collect from their children.
    - The online service must maintain data limits and reasonable security for the information it collects.
    - Each of these requirements have multiple sub-issues
- COPPA applies in two scenarios.
    - Actual knowledge: If an online service is a general audience site but it has some kind of registration and asks for age information. If someone signs up and indicates that they are under 13, the service provider meets the actual knowledge requirement.

    - Service directed to children either in whole or in a part: The FTC will look at several factors such as the nature of the service, the subject matter, characters, activities that appeal to kids, advertisements directed to kids. The FTC will also look at audience demographics if that is available.
    - There are different compliance standards for different types of targeted activities (directly to children under 13 or all individuals including those under 13).
- COPPA only applies to certain types of personal information collected by an online service but the definition is very broad (name, address, email, screenname, biometrics, geolocation, persistent identifiers, etc.)

COPPA consent

- COPPA requires online service providers to obtain verifiable consent from parents.
    - An online service must notify parents both on the website and in a specific direct notice.
    - The consent must be reasonably calculated in light of all the available technology to ensure the person providing the consent is actually the parent of the child.

***Question:** You've expressed that COPPA requires specific parental consent but schools can consent in specific scenarios. How does COPPA apply in the school context?*

Answer: There was a gap in coverage between FERPA and COPPA when schools began to use ed tech more frequently. The FTC issued a set of FAQs on this subject. These FAQ outline that it is the school district who is entering a contract with a service provider. In these cases, the schools are permitted to act as the parent agent only when the service is collecting student information only for an educational purpose. Once a service goes outside the educational purpose, they must obtain parental consent. Additionally, the service must provide all the COPPA required notices to the school as if they were the student's parents.

***Question:** Do you think there will be an increase in COPPA enforcement in ed tech that has ad tech?*

Answer: We are seeing that the FTC is very active in COPPA enforcement generally. The FTC recently put together a task force on privacy and harm. COPPA however, does not need the determination of harm to show a violation. The FTC has always considered children's data to be particularly sensitive. The agency is much more willing to go after actors who are using children's data for advertising. I think we will see a lot of new actions in this area.

***Question:** What are some best practices that you recommend around advertising technologies?*

Answer: I think practically speaking schools should make sure they are getting the right information about how student users will be tracked and who will see their information. I also think that schools should read and use the FTC's guidance on their website both in terms of how to provide notice to parents and what websites to use. There's one issue that we did not touch on: what happens when an app is used by a teacher and not by a school district. Teachers may not be savvy enough to properly comply with COPPA or FERPA.

One of the things that I would recommend is that school districts train their teachers on these issues.

Linnette Attai (PlayWell LLC) on State Student Privacy Laws and Ad-Tech

State student privacy law overview

- The last couple of years has seen a rise in state based student privacy legislation.
- Each state has its own unique regulatory environment when it comes to student data privacy but several key trends highlight commonalities among states.
- These include:
    - Parent & eligible student data control and choice over data use;
    - Transparency;
    - Being very specific on why data is collected;
    - Not using reusing data;
    - Minimizing data collection; and
    - Maintaining reasonable security.
- Many state student privacy laws also contain COPPA provisions and traditional advertising concerns.
- When advertising is involved many state laws prohibit using information to advertise directly to an individual student (in some states, the parent), prohibitions on profiling a student for advertising, reaffirming parental rights over student data, requiring deletion of data at the end of a contract, transparency, and reasonable security.

State student privacy model laws

- California's SOPIPA is the model state legislation that many states have adopt in whole or in part.
- SOPIPA began the trend of directly regulating service providers as opposed to FERPA's regulation of educational institutions.
- SOPIPA prohibits the use of personal information (covered information) from being used for targeted advertising on any site or service.

Challenges in state student privacy laws

- Many states have unclear definitions of important terms such as targeted advertising
- These definitions preclude use of a fairly broad range of student data that is personally identifiable.
- These laws also generally prohibit the creation of a student profile for advertising purposes.

Question: How do state student privacy laws and COPPA work together?

Answer: States may cover certain types of information that is not covered under COPPA such as persistent identifiers. Additionally, several state laws expand the definitions of personally identifiable information. Many service providers are familiar with COPPA but not with state privacy laws or FERPA.

Question: ***What are the recent COPPA enforcements that implicate ad tech?***

Answer: There have been some very interesting developments in ad tech enforcement that have happened in NY state. COPPA is enforced both by the FTC and states. Some states are very active in COPPA enforcement (including the FTC). There were four major players in recent actions, Nickelodeon, Mattel, Hasboro, and Jumpstart. These organizations were fined over $800,000 and were required to implement comprehensive reforms. Three of the organizations (Nickelodeon, Mattel, and Jumpstart) were required to provide regular reports on the results of their scanning. Hasboro was part of a Safe Harbor program which had no financial penalty.

- Nickelodeon had several third party advertisers placed tracking technology on Nickelodeon's websites. Despite Viacom's attempts to stop the tracking, the regulators believed that they did not act quickly enough to stop the tracking.
- Mattel had third party tracking provided by a third party data broker. Mattel was using tracking for site analytics. However, the tracking service provided by the third party introduced advertising tracking as well.
- Jumpstart had a situation with Neopets which was also using tracking technology for users who were logged in and other users as well.
- Hasboro had an issue with nerf websites which allowed users to be tracked across their website and allowed third-parties to retarget users with advertising off of their services.

These parties are all engaged in settlements and additional requirements because of their advertisements. These companies were not properly vetting their third party advertisers.

Question: ***What are some best practices that you recommend around advertising technologies.***

Answer: I think areas where schools are struggling the most is understanding how the ecosystem of services they are bringing into their system has been vetted in any way to ensure federal and state privacy law compliance. Teachers need to understand that when they click agree on apps or services, that is a contract. Most privacy training centers around security issues and ignore other areas around privacy areas. Most security breaches occur due to human error and not a problem with system security. I would encourage schools to look at the privacy toolkit we issued earlier this year.

Bill Fitzgerald (Common Sense Media) on Best Practices: Privacy Policies

Common advertising issues in privacy policies

- In reading through policies there is a broad range ways advertising is addressed.
    - Some policies are very clear on what third parties they use and what they do, including individual listings of the third parties with descriptions of what data is shared and for what reasons.
    - Other policies have very little to no information on third parties or what information is shared with third party vendors.
- Policies that are clear and specific is a good sign that a service is careful with student data whereas policies that are unclear as to what third parties are involved with the service should be a flag to schools and districts that student data is vulnerable.

What does it mean if there is a third party tracker on a site or service?

- At the most basic level if there is a third party tracker on a site or service that means that there is some tracking going on, but that doesn't tell the user all that much.
    - The first thing that someone curious about a third party tracker should do is to try and find out what that tracker is actually doing through a cookie manager or a intercepting proxy.
    - An intercepting proxy allows a user to look at all the traffic between the browser and a service and any third party involved.
- Generally, the vaguer and difficult it is to find out what third party is doing the tracking, that is a sign that more research on what that tracker is doing is necessary.
- The presence of a tracker on its own should not be taken as indication that something suspicious is going, it is merely an indication that more research should be done to figure out what the tracker does.

What doesn't it mean if there is a third party tracker on a site or service?

- When looking at a site or service the presence of tracker doesn't indicate tracking and the absence of a tracker doesn't indicate that service or site is not doing some kind of tracking.
- There are a lot of ways for a site or service to collect information behind the scenes.
- Service provided for free tend to have some tracking inherently involved and special scrutiny should be taken when using a free service.
- There is also a range of ways that users of a service may be tracked beyond the use of cookies. Likewise, tracking may not involve the use of personal identifiers.
- There are some systems that will collect plug-ins and other system information that may be used to identify users over time. Blocking cookies will not prevent this kind of tracking.

How can a user cross reference trackers on a site or service to what is disclosed in privacy policies?

- From a vendor perspective, school districts really appreciate have a clear policy that specifically lists how user information is used and what is tracked and shared with third parties.
- If the list of third party URLs on the website or service matches the ones listed in their policy that's a really good sign that the vendor really controls their service and understands what is happening on their system.
- There are some ad tech providers who will chain multiple requests together and these chains shift over time. Unless a ed tech vendor is actually monitoring what third parties get called, it's possible that tracking is occurring without the vendor being aware. It could potentially get the ad tech vendor in trouble.
- It is important for schools to get in contact with the technical people for any ed tech vendor and making sure that there is no disconnect between vendors and third parties.

***Question:** What are some best practices that you recommend around advertising technologies.*

Answer: Whether you are a vendor or a school district run your software through an intercepting proxy and see what turns up. We have written up a guide (listed in the resources) for how to set up a proxy. The common sense media website has lots of resources to help with finding best practices in these areas.

Attendee Question & Answer

When it comes to children and students monetizing the ad space on most websites with interest based advertising in most cases will not be legal in most circumstances. Where I think most people get hung up is when the ad tech company is interested in buying its own ads elsewhere on the internet or when the company is interested in understanding the effectiveness of their ads in general. Analytics seem to be okay under COPPA but possibly not under state law. Tracking your own ad effectiveness seems to be okay. What isn't okay is re-targeting ads. There is a technical cookie flag that can be sent when COPPA is indicated (when a user is a child) so that ad tech can disengage in targeting a user.

***Question:** How does retargeting ads work from a technical perspective and how does that play into COPPA and FERPA?*

Answer: There are about 7 or 8 different technical variants that are used, sometimes they are actually present in javascript, but when I'm look for these on what I can observe I just do direct searches for that. I generally use that as an indicator that there is a good faith effort to comply with COPPA. I would love to see a comprehensive framework that would explain exactly what the industry wide explanation of these technical flags are.

***Question:** Are there no legal limitations to using student data to serve advertising choices to parents, not students?*

Answer: This is very much dependent on the state laws, configuration of your product and what data is used to serve the advertising. For example, California's SOPIPA prevents use of any information collected or obtained as a result of use of the product to serve targeted advertising, both on and off the service in question. Some state laws specifically preclude use of student data to target advertising to parents or students, while others are particular to precluding advertising to students. In addition, when embedding ads on your site, service or platform, ensure that your configuration strictly limits data use, tracking and retargeting to the adults and doesn't "leak" into sections used by children/students. You want to look very carefully at what state laws say. Be very careful when embedding ad tech to avoid misconfiguration that may inadvertently target student users.

Answer: A quick and easy check for whether embedded ad tech targets students is to create test accounts for different user types and compare what user types experience.

***Question:** Where did these end with Google and FTC action from years ago with the EFF privacy complaint alleging that google was violating the Student Privacy Pledge?*

Answer: The FTC doesn't confirm or deny the existence of its investigations so who knows. When groups like EFF file FTC complaints they generally look very legalistic and formal but the FTC is under no obligations to respond or take any action. FPF, as one of the creators of the Student Privacy Pledge, disagreed with any violations and most

people did not think Google was violating the Pledge. The EFF complaint felt incomplete, inaccurate, and misleading. There were elements within the EFF complaint that didn't reflect how technology was being used in schools and the ability of even a moderately skilled school administrator to take care of things. This is the type of thing that makes doing good advocacy work difficult.

***Question:** How can a school district keep up with all the terms of service and privacy policies of online tools?*

Answer: There's probably between 300 and 400 applications that are used by 90% of students. Getting coverage over those primary applications will help ensure that everyone can make informed decisions about how technology can be used. It is critical to have conversations like this because we need to be able to communicate about this because the landscape is always changing.

Answer: This is the job of a chief privacy officer or a privacy team. It's not something that can just be picked up as an additional responsibility. Vendors and schools need to become very familiar with what is negotiable and non-negotiable in contracts. Don't be afraid to ask questions or have open conversations. Everyone is struggling with it and there are no easy answers.

Audience Questions Answered in Google Doc

***Question:** How can you tell if a website has ad trackers?*

Answer:

- Use "Ghostery"/Evidon Browser extension
- TrustArc, Evidon and others offer a service that makes it possible to see if a website has ad trackers
- Holland & Knight offers sophisticated proxy analysis for sites, services and connected devices that go deeper than many consumer tools (although those are very useful!), along with legal analysis of the findings

***Question:** Are there reasonable methods to permit an EdTech company to engage in retargeting for adult website visitors but not for child visitors?*

My understanding is that Google's Tag for Child Directed Treatment tools can be applied to a particular ad request on a publisher site or to the entire publisher site, but that the TFCD feature is not effective for advertiser sites wishing to halt interest-based retargeting of their ads shown on a third party site. I would be interested to hear if the panel has practical advice or tips for retargeting on a mixed audience (adult/student) site.

Answer: Using child-directed signaling (when offered) is one way, but it is not a cure-all. It is critically important to know what information your third parties are collecting, how they're behaving and to have contractual controls in place (see answer to question 5) below. In addition, I cannot stress enough the importance of embedding the code properly! Companies often get caught up when they *think* they are only targeting and retargeting adults, but the configuration allows targeting and retargeting of everyone. (Linnette Attai, PlayWell, LLC)

***Question:** What are the rules for opt-in advertising by students/parents?*

For example, when a student takes the ACT, they actually have to opt out from having their information shared with higher education institutions. The SAT is an opt-in process. Can you go into details around the legalities of this and how companies like ACT/College Board can legally justify having minors make this election?

Answer: As with the question above, it's important to look at state student data privacy laws, some of which preclude all targeted advertising, and some of which only preclude targeted advertising when directed to students. Some, including SOPIPA, do not include an exception to allow parents to opt-in or otherwise consent to targeted advertising to their students. With respect to ACT/College Board, they are often afforded exceptions in the state laws. For example, Texas recently passed a student data privacy law that makes exceptions to the preclusion against targeted advertising, and against selling or renting student information for, "a national assessment provider if the provider secures the express written consent of the student or the student's parent to provide access for the student to employment, educational scholarships, financial aid, or postsecondary educational opportunities." Texas is not the only state to include this type of exception for ACT/College Board. (Linnette Attai, PlayWell, LLC)

***Question:** Are the advertisements on YouTube Kids compliant with COPPA and FERPA?*

Answer: YouTube Kids app is designed with the intention of being compliant with COPPA. YouTube.com is not. However, on the app, there is advertising that is pulled in. While it may be missing the trackers that are present on the website, there were concerns, when the app first launched, that the advertising was not appropriate. Google has done a good deal of work on that since then, but it's worth reviewing to ensure it's in line with your expectations of appropriateness. Also, I recommend looking at the fairly extensive parental controls within the app, that would allow the parent or teacher to set a timer on viewing and limit where the child can search for content, which helps to create a more walled off, appropriate experience. YouTube Kids does not require that users provide PII, so it *should* be in line with FERPA requirements. (However, please note that this is not reflective of an official assessment.) Only the school can ultimately determine if the app may be used in compliance with your school's expectations around FERPA. (Linnette Attai, PlayWell, LLC)

***Question:** There are so many third-party tags other than advertising that could potentially be issues here, social sharing, analytics, video serving, etc. Should vendors be concerned here as well?*

Answer: Yes, absolutely! Whenever a vendor is engaging with a third party, the vendor is responsible for ensuring that the third party operates in compliance with the laws. With respect to COPPA, there is some shared responsibility if the operator has actual knowledge that they are operating on a site or service intended for children, but in most cases, when it comes to social sharing, analytics, video serving, etc., these third parties are embedded without actual knowledge on the part of the third party, so the vendor is strictly liable. Regardless, keep in mind that the vendor will never be off the hook. It's your product. You are responsible. When it comes to FERPA and state student data privacy laws, third parties are much less likely to even be aware of the education technology ecosystem or the laws that apply. The vendor needs to know what third parties are operating within their site or service, what information the third party receives

and why, what they do with it, and how the third party protects the information (in compliance with applicable laws, the vendor privacy and security practices and the school or district expectations). (Linnette Attai, PlayWell, LLC)

***Question:* FERPA is a law for schools to follow, not edtech vendors. This message should be conveyed to school districts that constantly hound vendors to make sure we are FERPA compliant when they need to be.**

Answer: FERPA is a law for schools, but if an ed tech vendor operates in a way that causes a school district to fall out of compliance with FERPA, the district would be precluded from giving the vendor student data for a period of 5 years. (And in today's climate, expect that would cause problems for the ed tech vendor across the country.) So, while I agree with you that when a school district asks a vendor if they are "FERPA compliant," it is a meaningless question, as it is when vendors assert that they are "FERPA compliant" in an attempt to provide some comfort to schools, it is imperative that ed tech vendors operate in alignment with FERPA and support school compliance with FERPA by ensuring that their product can be used in a manner that keeps the school in bounds of the law. Also, keep in mind that many of the state student data privacy laws are set up to be enforced directly on the vendor. (Linnette Attai, PlayWell, LLC)

***Question:* COPPA is a law for vendors to follow, not schools. This message needs to be conveyed to vendors.**

Seems that at least 50% of the agreements I read state that schools/teachers/district are responsible for COPPA compliance. COPPA is administered by FTC, directed at commercial vendors and contains requirements that a school/district/teacher couldn't possibly guarantee, even if they wanted to.

Answer: Correct: the only part of COPPA that the school/district might be responsible for is obtaining consent in lieu of the parent. That can only happen when a) there is a contract in place (and remember that a click-wrap is a contract) and b) when the data is used for the school purpose and for no other commercial purpose. All other COPPA obligations fall to the vendor. (Linnette Attai, PlayWell, LLC)

***Question:* If I am a member of a school and it wants to "advertise' or 'promote' opportunities (college choice, scholarships, etc) does this fall into "advertising" or a "service" provided by the school? Same question but for an alumni of same school.**

Answer: Advertising is advertising. There is no ban on advertising. So it depends: what information are you using to serve the advertising? If student data (including persistent identifiers) are used to serve the advertising, consult the state laws, PPRA and COPPA (if for users under 13), as this is where the preclusions kick in. In addition, if the service is designed to help students search for colleges, scholarships, etc. - if that is the point of the product and the data is used appropriately, within the bounds of privacy laws - this can also be within bounds of the laws. Also, note that several state laws have exceptions to their advertising restrictions that specifically permit surfacing information on colleges, scholarships and in some cases, employment opportunities to students. (Texas, Utah, Colorado and possibly North Carolina are some that have passed permissive language.) (Linnette Attai, PlayWell, LLC)

Question: ***Now that ISPs can gather information on their users are they no longer COPPA or FERPA compliant? Can the ISP use or sell this information to others under the new law for under and/or over 13 year olds?***

Answer: The protections against ISPs selling data were never actually in place (the law wasn't active before it was repealed). Your agreement with your ISP provider should include the necessary provisions to prevent them from selling the data. One permissive law (or lack thereof) does not negate requirements of other laws. Check your agreement for the right protections. (Linnette Attai, PlayWell, LLC)

Question: ***For COPPA purposes, how do you draw the line between a general audience website/app when it includes, e.g., cartoons/characters and other imagery that are themselves generally aimed at children? I.e., how do regulators determine when the nature of the website changes from general to children-oriented?***

Answer: COPPA determination of whether or not a site or service is directed to children is laid out in the law. It is a "totality of circumstances" test, that encompasses the look of the site, whether or not it includes animation, celebrities that may appeal to children (and keep in mind that the FTC has said that celebrities like Rihanna appeal to children, so the bar there is high). Also considered are what advertising you run on the site or service, where and how you promote your site or service and more. No one factor is more important than another. Your intended audience is of interest, but tends to not be very important in practice. See the FTC COPPA FAQs (in the Resources list, below) for the complete list. I often tell companies, "if it looks like it's for kids, or feels like it's for kids, it's for kids." Be very careful in making the determination that it is not directed to children when your site or service hits on some of the COPPA factors of "directed to children" and not all. The regulators may not see it the same way that you do. (Linnette Attai, PlayWell, LLC)

Question: ***The Terms of Service that say "I verify I'm over the age of 13…" done by countless mobile app companies are all in violation of COPPA then?***

Answer: Not necessarily, as it depends on whether or not the site is directed to children as that determination is made under COPPA. The FTC is going to look at the site or service to determine whether or not it is directed to children, and if it is, in whole or in part, the vendor isn't permitted to screen out younger children by age. Sometimes I see this "I verify…" statement when a vendor confuses the laws, and really means to say, "I verify that I'm 18 or older," as in "This contract will be legally binding." (Linnette Attai, PlayWell, LLC)

Question: ***Re FERPA - I get that use of PII not permitted for advertising purposes. What about use of de-identified data for advertising?***

Answer: FERPA is not specifically permissive on advertising, but does allow de-identified data to be shared without parental/eligible student consent. However, by contract, schools don't have to allow vendors to use de-identified data for their own purposes (although many vendors simply can't accommodate such requests - it can be extremely difficult to wall off one school's de-identified data from another's - it all gets aggregated into one big bucket). State student data privacy laws permit use of de-

identified data for very limited purposes, none of which include advertising. (Linnette Attai, PlayWell, LLC)

Question: ***What are the rules or guideline around a school using a service like facebook or twitter? The school does not own the student's account (though they may encourage them to sign up for an account) and the student then must friend/follow the school. However the student can now be advertised to. Is this allowed?***

Answer: I would first question why a school would encourage a student to sign up for a Facebook or Twitter account. However, remember that there is not a ban on advertising to students. There are preclusions against behavioral targeting to children under 13 and preclusions against targeted advertising when the targeting uses data collected as a result of the use of the ed tech product. Having said that, if a student uses Facebook or Twitter, those platforms may advertise to those individuals. Facebook collects age, and precludes users under 13 from registering for the platform, and they are allowed to advertise to their users. (Yes, there are underage individuals there, but that's a conversation for another day)! (Linnette Attai, PlayWell, LLC)

Question: ***Regarding data deletion policies in federal and state laws and regulations, what is a good way to reconcile requirements to delete PII at the end of a contract with requirements I often see from schools and districts stating that we must retain all data beyond the duration of the contract (e.g., I saw one just today that stated a minimum of 6 years from the creation of the student account and at least 1 year after the student's graduation)? We hope to service all of our schools for that long but customers come and go for many reasons.***

Answer: Very dependent on your product or service. If you are a platform of record for a school, perhaps that is something you want to accommodate, but I would never suggest holding data past a contract term. What rules would apply? It is detrimental to both the vendor and the school to have the vendor holding data beyond the duration of the contract. (The school needs "direct control" under FERPA. Without the contract, there is none, so it may be worth reminding them of that.) In short, determine your retention period - how long can you reasonably, safety and securely hold the data. Ensure that the school has a way to access and download their data before you delete it, or that you will return it. Ensure that your retention period complies with state laws (some of which require deletion when the contract ends). And my recommendation is do not hold data when you don't have any legal agreement covering your rights to do so. So if you want to hold the data, have that be a provision of your contract - that you'll keep it after the school is done using the service, and under what terms. (Linnette Attai, PlayWell, LLC)

Question: ***More and more groups are making sites that are rating software/services relative to how they are in protecting student data. What are thoughts on protecting companies from misleading claims that can negatively impact revenue (i.e. rating on student data privacy based on third hand information rather than working directly with the company to actually learn their policies, procedures, terms, conditions, etc.)?***

Answer: Personally, I always am concerned about any rating service that doesn't make the way/process it uses to rate companies public (such as Common Sense Media's list of the questions they ask for ratings) or doesn't work directly with companies to find out how their processes work. I know of many companies with great privacy practices who

may not be great at communicating about those practices, so it is almost impossible for an outside rater with no access to tech info to accurately rate company practices unless they are doing an in-depth screening like CSM. (Amelia Vance, FPF)
Answer: I echo Amelia's comments here. And schools and districts need to understand that not all ratings and assessments are created equally. "Privacy" is a hot topic, and there are players coming into the space providing "solutions" to schools that are not backed by data privacy and security experience.

- Schools: no matter what, there is no such thing as a third party assuring you that a vendor is compliant with the laws. That is between you and the vendor. The pledge is a solid assertion of a vendor's behavior, and CSM makes their process transparent (and it's run by someone with deep knowledge on the subject). These are tools that you can use in getting started.
- Vendors: to protect yourself from misleading claims, there is nothing to prevent you from publicly explaining why those claims are incorrect and the faulty basis on which those claims were made, if you get no direct relief from those making the claims. (Linnette Attai, PlayWell, LLC)

***Question:* Has the Dept of Ed imposed a 5 year ban (or any other ban) on ed tech vendors for FERPA concerns?**

Answer: No. (Sara Kloek, Department of Education)
Answer: At the Student Privacy Bootcamp FPF just did, the Department of Ed mentioned that they have been focused on releasing extensive technical assistance to SEAs/LEAs/vendors, but are now turning to enforcement - so a ban may be coming. (Amelia Vance, FPF)

***Question:* Bill Fitzgerald mentioned how some companies are very good about disclosing their third parties in privacy policies (e.g., type of 3rd party, what type of data shared, trackers, etc.). Are there any examples of a thorough such policy/set of disclosures, which can be reviewed as a possible model to work with internal technical teams on?**

Answer: Quizlet actually has a really interesting new privacy policy where they list out every third party they work with and what those third parties do. (Amelia Vance, FPF)
Answer: COPPA requires that third party operators be disclosed in the vendor's privacy policy, although may do not, and even in recent enforcement action, this is not an item that was addressed. However, the FTC recently re-issued its guidance on business compliance with COPPA, and this requirement was included, so we can hope that operators will take notice. I imagine we'll see more of these disclosures in the future. (Linnette Attai, PlayWell, LLC)

***Question:* Does anyone know a vendor that will review privacy policies and TOS for districts?**

Answer: There are a few consultants that do this really well (Linnette is one), but see the answer to Question 16 - it is very difficult to do. I recommend 1) looking to see if a vendor has signed the Student Privacy Pledge, which is an indication that they are (at a minimum) thinking about student privacy; 2) looking to see if Common Sense Media has rated them (which is a more in-depth review, including a look at security from the outside); and 3) looking to see if the vendor has signed a contract with a state in the Student Data Privacy Consortium (where you can see if they signed a special contract

addendum on privacy). Especially for small districts, rely on big districts like Denver Public Schools, Cambridge Public Schools, and Ventura County Public Schools, which all have AMAZING privacy programs and you can assume they have done due diligence on the ed tech products they are using. (Amelia Vance, FPF).
Answer: Please feel free to contact me as well - happy to help with review or just discuss informally and give you some tips for implementing a review program in your school or district that fits within the manpower you have available to help get you started. (Linnette Attai, PlayWell, LLC)

On the call there was mention of the school acting as the agent of a parent to comply with COPPA (i.e. the "school consent") which is limited to just educational context. However, you will see that in the COPPA FAQ's themselves that there appears to be even an internal inconsistency if school's themselves should get direct consent from parents (as opposed to acting as their agent). You also see companies like Google, etc. having sample "school consent" forms that are in fact forms for teachers to get individual parental consent.

***Question:** Is it just best practice to do these parent consent forms as a teacher?*

Answer: There are requirements for the vendor when it comes to COPPA, one of which is ensuring that parental consents are obtained from the parent, legal guardian, or school acting in lieu of the parent before the data is collected, and when the data is only used to serve the school purpose and for no other purpose. The vendor can assume that you have the consents in place if you have a contract (including a click-wrap), however they must provide you with the required notices, which the FTC encourages schools to make available to parents. You need to determine if you need to get new consents, or if you have already obtained them - perhaps within other consent forms you have sent home to parents around use of technology in schools. It is always good to have consent forms. However, actually getting them can be a complex proposition. Remember also, that even if you cover off on COPPA requirements, FERPA requirements and state student data privacy law requirements still apply. (Linnette Attai, PlayWell, LLC)

Recommended Resources

1. Advertising in Schools from the Data & Society Research Institute
2. U.S. Department of Education's (new!) student privacy website
3. Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices from the U.S. Department of Education
4. Basic Information Security Primer: https://github.com/billfitzgerald/infosec-primer
5. FTC FAQ's on COPPA: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions
6. FPF Guide to Student Data Protections Under SOPIPA https://fpf.org/2016/11/07/fpf-guide-student-data-protections-sopipa-k-12-school-administrators-ed-tech-vendors/
7. Additional questions on FERPA, PPRA, or general best practices on student privacy may be directed here: https://studentprivacy.ed.gov/contact.
8. Protecting Student Privacy While Using Online Educational Services: Model Terms of Service from the U.S. Department of Education
9. CoSN Protecting Privacy in Connected Learning Toolkit

10. Vendor information from Common Sense: https://www.commonsense.org/education/privacy/about/vendors

Attending Organizations

Please email Amelia Vance at avance@fpf.org if you were on the call and your organization name is not listed below.

1. 5-Star Students
2. Aequitas Solutions
3. Age of Learning, Inc.
4. AisleLabs
5. Allegheny Intermediate Unit, University of Pittsburgh
6. Amazon
7. Amplify
8. Bloomz
9. California Department of Education
10. Cambridge Public School District
11. Classcraft Studios Inc.
12. Classworks
13. Colorado Department of Education
14. Comcast
15. Common Sense Media
16. Conversant
17. Council of School Attorneys, National School Boards Association
18. Denver Public Schools
19. Desire2Learn (D2L)
20. Edmentum
21. Edmodo, Inc.
22. EDPuzzle, Inc.
23. Education Week
24. Educause
25. EduTone
26. Epsilon
27. EverFi
28. Facebook
29. Flyer School App
30. Gaggle
31. GoGuardian
32. GradeHub
33. Gradescope
34. Hillsborough County Public Schools
35. Houghton Mifflin Harcourt
36. IAPP - International Association of Privacy Professionals
37. iKeepSafe
38. Illuminate
39. Imagine Learning

40. Interactive Health Technologies
41. Khan Academy
42. Lifetouch, Inc.
43. Loeb & Loeb
44. Los Angeles USD
45. Loudoun County Virginia Schools
46. McGraw-Hill Education
47. Mehlville School District
48. National Student Clearinghouse
49. Netflix
50. New York State Department of Education
51. Nissen Consulting
52. Northshore School District
53. OnCourse Systems for Education
54. Orrick
55. OverGrad
56. Pearson
57. PlayWell, LLC
58. Potomac Technology Law + Policy
59. SchoolInfoApp
60. SchoolMessenger
61. Sidley Austin
62. Skoolbo
63. Streetlight Data
64. trovvit
65. TrustArc
66. University of Michigan
67. Utah SEA
68. Ventura County, CA Office of Ed
69. Wilson Sonsini Goodrich Rosati
70. Yahoo! Inc.
71. zeotap GmbH