



Transcript: Protecting Student Privacy While Using Online Educational Services: Model Terms of Service

Slide 1:

Baron Rodriguez: Hello. And welcome to the joint presentation with the U.S Department of Education and its Privacy Technical Assistance Center, or PTAC. Today, we are pleased to provide an update based on the Department's newest guidance: Protecting Student Privacy While Using Online Educational Services: Model Terms of Service. My name is Baron Rodriguez, and I lead the PTAC Center. With me is Shane Morrisey, the Privacy Advisor for the U.S. Department of Education.

Slide 2:

Baron: To start, we want this to be a webinar enjoyable to all, so phone lines will be muted. Throughout the webinar, we will have interactive polls which should pop up during the presentation. As always, our webinars are recorded and will be posted to the website within a few weeks. All citations we discuss today will also be available in the new guidance document.

Slide 3:

Baron: Due to the potential number of participants, we request you type any questions in the lower right hand corner of the webinar window. We will get to as many as we can, and please keep in mind some questions may not be answered today, but may be forwarded to the PTAC helpdesk for further review.

Slide 4:

Baron: In our webinar today, we will discuss online educational services, the student privacy landscape, click-wrap agreements, and good/bad privacy related terms of service provisions.

Slide 5:

Baron: Our goals today are: 1) to provide some information about the current state of the student privacy landscape and how that affects our terms of service analysis, 2) to provide information about what it means to accept a provider's terms of service, and 3) to equip school officials with the tools needed to analyze privacy-related terms of service provisions you'll probably see from providers.

Slide 6:

Baron: Because of the complex and changing nature of classroom instruction the Privacy Technical Assistance Center has authored this new guidance to help schools and districts evaluate Terms of Service Agreements.



Slide 7:

Baron: This guidance examines provisions to privacy that may be found in a Terms of Service, privacy policy or other contract offered by a provider of online education services or mobile applications. Some examples include classroom applications downloaded on to handheld devices, supplemental applications purchased by districts or schools, and free applications. This guidance does not cover online services or social media used in a personal capacity. Further, this guidance does it apply to school services that are not accessed by parents or students, such as a system used by administrators or teachers.

Slide 8:

Baron: There are so many classrooms now utilizing services, games, and applications offered by 3rd party providers. This is great...BUT this has led to increasing concern about the commercialization of student information and behavioral marketing. The data that results from using these services needs to be used effectively, appropriately, and in a manner that protects student privacy

Slide 9:

Baron: There are several Federal statutes that implement privacy protections throughout various subject areas. The Family Educational Rights Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and the Children's Online Privacy Protection Act (COPPA) are the major laws that govern student privacy.

Slide 10:

Baron: Student privacy has been a hot topic in state legislatures. During the 2014 state legislative season, over 100 bills related to student privacy were introduced throughout the country. As of February this year, 102 bills have already been introduced!

Slide 11:

Baron: One of the biggest student privacy bills passed at the state level last year was the Student Online Personal Information Protection Act (SOPIPA). This law will establish obligations for providers and restrictions on how student information is used. There has been a lot of talk about the introduction of a federal bill based on this law.

Slide 12:

Baron: Independent privacy groups started a pledge for K-12 service providers to help secure the privacy of the collection, maintenance, and use of student personal information. This pledge has even been endorsed by President Obama. Providers who fail to meet the standards established by the pledge would be subject to potential enforcement actions by the FTC, or Federal Trade Commission.

Slide 13:

Baron: There have been recent congressional hearings which have discussed amending FERPA. Various changes have been discussed including: expanding the definition of an "education record," enforceable penalties for FERPA violators, and implementing new data security standards.



Slide 14:

(Poll 1): What types of participants are in the audience today? Please indicate which sector you represent:

- K-12 Administrators
- K-12 Teachers
- Postsecondary administration or faculty
- Education technology industry
- Other (e.g., parent/student, non-profit org., etc.)

Slide 15:

Baron: Before we get to some Terms of Service provisions, let's quickly review some FERPA obligations, so we know what information can be shared with providers. What does FERPA require if PII, or personally identifiable information, from students' education records is disclosed to a provider?

Slide 16:

Baron: Either parental consent will be required for the disclosure, or the disclosure must fall under one of FERPA's exceptions. The most common exceptions used are the directory information exception, or the school official exception. When talking about online educational services, providers will most often be allowed access to student information under the school official exception.

Slide 17:

Baron: If providers are allowed access to student information, in what ways are the uses of that information limited?

Slide 18:

Baron: Under the directory information exception, there are no limitations other than what is included in the school or district's agreement with the provider. Under the school official exception, PII from education records may only be used for the specific purpose for which it was disclosed, and providers cannot sell or share PII except as directed by the school or district and only as allowed by FERPA. The PPRA may also apply, which places limitations on the use of student information for marketing. And now we'll turn it over to Shane who will talk more about Terms of Service.

Slide 19:

Shane: Thanks Baron. The Model Terms of Service Guidance analyzes sample privacy-related Terms of Service provisions. This analysis will take into account federal privacy laws and privacy best practices. Bear in mind that the relevant agreement offered by a provider may not be called "Terms of Service". It may also be called a "Privacy Policy," "Online Service Terms," or something else. But regardless of what it is called, this guidance will help you navigate these agreements and help you decide what is best for your school or district.



Slide 20:

Shane: A traditional contract involves a buyer and seller agreeing on a set of terms and signing based on those agreed upon provisions. However, this is not the case with click-wrap agreements, which are used by many providers of educational services. Baron, when you want to get that new “zombie racing game” for your tablet, do you get the opportunity to negotiate the terms of service with the company providing the game before you download?

Baron: Of course not! Who has time to read pages and pages of legalese? There aren’t even phone numbers or points of contact that can be used to contact the company and negotiate. I just click “I agree” so I can start playing.

Slide 21:

Shane: Click-wrap agreements are not negotiated, so a school or district is pretty much left with a “take it or leave it” situation. If you are a representative of a school or district, it’s important to remember that when you agree and use an application in the classroom, you are agreeing on behalf of the district, and depending on the information the application collects and how that information is used, you could be in jeopardy of violating privacy laws.

Slide 22:

Shane: As I mentioned earlier, agreements that are not negotiated are referred to as “click-wrap” agreements. Once agreed to, these agreements can serve as a legally binding contract between a provider, and a school or district. They will likely govern what information a provider can collect, and what the provider can do with that information.

Slide 23:

Shane: Most importantly, these click-wrap agreements could potentially lead to a violation of FERPA and/or PPR, and, also, may not exemplify privacy best practices.

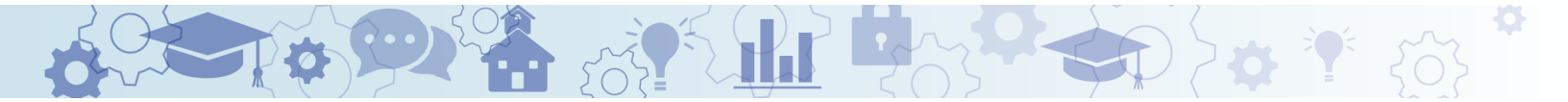
Slide 24:

Shane: A good practice that can help avoid privacy law violations is to implement a policy for the review of agreements before a service is used in the classroom. Baron, have you ever worked in a place where you aren’t able to download software without IT or management approval?

Baron: Nope, everywhere I’ve worked has had an established policy in place that must be followed in order for software to be downloaded in the workplace. For some reason, the idea of free applications on smart devices such as tablets and phones has usurped that review process. Much like computer software, there are licensing, privacy, legal and yes, even virus considerations that may factor into these free applications.

Slide 25:

(Poll 2) Familiarity with TOS: How many of you have actually read an entire agreement before clicking “I agree”?

- 
- Of course!
 - I skim.
 - Honestly, no.
 - I tell people that I do, but I'm actually lying.

Slide 26:

Shane: We will now begin discussing example Terms of Service provisions and how those provisions can impact the security of a student's privacy. Remember that every agreement will have different language, but hopefully the examples we discuss today will be close enough to the provisions you will actually see to help you make an informed decision about whether or not to use an educational service.

Slide 27:

Shane: Usually Terms of Service will begin with a Definitions Section. This section will define terms that will be used throughout the agreement. The manner in which certain terms are defined can have a big impact to the privacy protections laid out in the Terms of Service. When defining student data, the more broad a definition is...the better. Use caution if there is a narrow definition of "data." This could leave a lot of student information unprotected by the agreement.

Slide 28:

Shane: Even though we've been using the term "data," that will not always be the term that is used to refer to information about students that is collected, used, or shared by a provider. Some other common terms are "Student Information," "Student Data," or "Covered Information"

Slide 29:

Shane: There can be a lot of data available to the providers of educational services that can be collected and analyzed. This includes "Metadata" which can be defined as data that describes other data. Examples include: Mistakes by a student playing an online math game, the amount of time it takes a student to complete a given task in an app, and even the number of mouse clicks that are made. All this can be collected and analyzed to help improve a product and enable a provider to create more effective educational services

Slide 30:

Shane: With all these data being collected, it's important that student privacy is maintained. Even when direct identifiers have been removed (such as a student's name or ID number) it can still be possible for that information to be re-identified. Removing not just a student's name or ID number, but also removing date of birth, demographic info, location info, and school ID can help ensure the data are truly de-identified

Slide 31:

Shane: Even if all the identifiers I've just discussed have been removed it could still be possible for that information to be re-identified. That's why it's a best practice for providers to include a commitment to not re-identify data within their Terms of Service



Slide 32:

Shane: Providers could potentially use the information they collect to create a profile on a student. That profile could then be used to send targeted advertisements or marketing materials to that student.

Slide 33:

Shane: A good Terms of Service will make it clear that advertising to students is not allowed. Targeted Advertising or marketing could violate privacy laws.

Slide 34:

Shane: Terms of Service often include a provision for the modification of the Terms of Service. Many providers may try to allow material changes to be made without giving notice to the school or district. A provision that agrees to give notice of Terms of Service modifications is good...a provision that agrees not to modify without the consent of the school or district is better.

Slide 35:

Shane: Data that are collected should be limited to only what is necessary for the provider to offer the educational services laid out in the agreement. The absence of a provision that places restrictions on data collection could allow for the unrestricted collection of a wide array of student information. Something to look out for, would be provisions that view accessing a provider's services from another 3rd party website as an exception to the limitations set forth in the agreement.

Slide 36:

Shane: Limiting what providers can do with data will help schools and districts fulfill their obligations under FERPA by maintaining control over the use of student information. Be on the lookout for provisions related to data use that contain the phrase "without providing notice to users."

Slide 37:

Shane: Providers often perform "data mining" or other large-scale analyses of data to improve the features of their educational products and services, or to learn more about those who use their service and how they interact with it.

Slide 38:

Shane: If a provider is going to perform data mining, the uses for this practice should be explicitly spelled out in their terms of service. Data mining of student information for the purpose of targeted advertising to a student or parent should be prohibited

Slide 39:

Shane: It's very common for providers to use subcontractors. And while sharing data with a subcontractor is acceptable, it's important the provider is transparent about what data are being shared and what is being done with those data.



Slide 40:

Shane: Providers should identify subcontractors who receive student data (either upon request, or as agreed to in their contract), and the school or district should consent prior to data being shared. Additionally, subcontractors should be subject to the same provisions contained in the provider's TOS.

Slide 41:

Baron: Thanks Shane. It's very important to remember that the Terms of Service agreement should retain the school or district's right to have student data destroyed or returned to them upon request or upon the expiration of the agreement. In addition, as a privacy and security best practice, data return or destruction helps limit the amount of personally identifiable information available to outside parties and prevents improper disclosure.

Slide 42:

Baron: It is also important to remember that student data is the property of the school and district, and you maintain the ownership of that data. There are some Terms of Service provisions that give providers exclusive and irrevocable license to student data. This can be a cause for concern and it should be noted that if a license is granted, it should be limited and only allow use of the student data for the educational purposes outlined in the agreement.

Slide 43:

Baron: FERPA does require schools and districts to make education records accessible to parents. To fulfill FERPA requirements, providers should be aware that they need to make student data available upon request, however to ensure that the identity and validity of the parent asking for the student information is legitimate, it would be a best practice for the providers to pass on the data directly to the school district.

Slide 44:

(Poll 3) What is your policy for reviewing TOS for your school/district?

- We have a policy to review agreements for online educational services and applications, and I know what that policy is.
- We have a policy, but I'm not sure what is involved or who does the reviewing.
- I don't know.
- We do not have a policy for reviewing these agreements

Slide 45:

Baron: In addition to the data access controls, consideration should be made to security controls in place within the agreements. Student data should be protected and providers' Terms of Service should include provisions outlining strong policies safeguarding these data. Failure to provide adequate security could lead to a FERPA violation. For more information on FERPA's reasonable methods, please visit our website at <https://studentprivacy.ed.gov>.



Slide 46

Baron: Our guidance document is available at this link along with other helpful guidance and tools, including a data breach response toolkit exercise and checklist.

Slide 47:

For additional information on these topics and best practice recommendations, please visit our websites:

- Family Policy Compliance Office (FPCO): <https://studentprivacy.ed.gov>
 - Provides detailed guidance on legal requirements under FERPA and PPRA.
- Privacy Technical Assistance Center (PTAC): <https://studentprivacy.ed.gov>
 - Provides guidance documents, trainings, checklists, frequently asked questions, and other resources relating to best practices for data privacy and security.

Slide 48:

Baron: Thank you for attending today's webinar. We hope that it has been a valuable use of your time. As always, we appreciate feedback and would like to hear about what you learned, what issues still need clarification what we can do better and any general feedback about our technical assistance efforts. At the conclusion of this webinar, you will be given a survey about this webinar. Please take a few minutes and provide feedback.