Transcript for the "Protecting Student Privacy While Using Online Educational Services" Webinar

Slide 1:

(Baron Rodriguez)

Hello, and welcome to our webinar entitled, "Protecting Student Privacy While Using Online Educational Services." My name is Baron Rodriguez and I am the director of the Privacy Technical Assistance Center, or PTAC. With me is Michael Hawes, the Statistical Privacy Advisor at the U.S. Department of Education.

(Michael Hawes)

Good Afternoon, or for those of you out on the west coast, Good Morning!

Slide 2:

(Michael)

Before we get started, I'd like to cover a few logistical items with you: One, phone lines have been muted. This is so all participants can enjoy the webinar without the crackling of phone lines or the inevitable elevator hold music. Two, we will be having interactive polls to get to know the audience. We look forward to your input. Three, the recording of this webinar will be made available on PTAC's website in approximately one week. And finally, in order to simplify this presentation, legal citations are not in the webinar, however will be available within the official guidance document.

Slide 3

(Baron)

If you have questions, please type them in the lower right hand corner of the webinar window. At the conclusion of the webinar, we will have a moderator answer a few select questions. We may not be able to answer all of your questions, either due to time constraints, or simply because we don't know the answer at this time.

Slide 5

(Baron)

The ever-changing landscape of technology is difficult to keep up with at best. PTAC/The Department recognizes that there is a need for more guidance around protecting student privacy in an electronic age. Remember that FERPA was enacted well before the preponderance of electronic data files and student information systems. As such, FERPA is very unclear around the protection of electronic student records. Today we are going to discuss, at a high level, guidance to help schools, districts, service providers, and others to navigate the best practice considerations for protecting student privacy. Remember that there *are* legal protections for student information used online and you should also consider state, local, and tribal law protections of student information as well. Finally, it's important to

think beyond simply being compliant with FERPA. We always recommend employing best practices in addition to compliance requirements such as PPRA and FERPA.

Slide 6:

(Michael)

Before we move on, we wanted to share this quote from Arne Duncan with you that was given at a recent conference: "We must provide our schools, teachers, and students cutting-edge learning tools. And we must protect our children's privacy. We can and must accomplish both goals..."

Slide 7:

(Baron)

Technology is everywhere in the education community. These are some examples of technology in schools that may contain or use student personally identifiable information, or PII. Student Information Systems such as Pearson or eScholar, Productivity applications such as Google Apps for education or Microsoft 365, educational applications such as teacher dashboards and fundamental school services such as school transportation services or cafeteria services.

Slide 8:

(Baron)

This particular guidance relates to the following subsets of education services such as computer software, mobile applications, or web-based tools that are provided by a third party, are accessed via the internet by students and/or parents, and are used as part of a school activity. This guidance is not covering online services or social media used in a personal capacity or those that are used by the district in an administrative function that are *not* accessed by parents or students.

Slide 9:

(Michael)

With the changes in the computing and telecommunications sectors over the last couple decades, we've seen corresponding shifts in these technologies' use in the education sector. This has led to a number of new privacy and data governance challenges that schools and districts have had to address. For starters, the growing complexity of many of these technologies, coupled with budgetary constraints, has led many schools and districts to contract out a greater share of school functions, rather than performing them in-house. As more services move online, and as technology advances, we have many new types of data that are being collected, and a whole lot more of it, overall. Many online services also increasingly use a "take-it-or-leave-it" Terms of Service agreement (often called a "click-wrap" agreement) instead of the two-party written contract model used in more traditional contracting relationships, which raises new challenges that we'll talk about later in the presentation. Faced with all of these developments, our

major challenge is to find a way to leverage the tremendous potential of these new technologies and data in an effective and appropriate way, without compromising students' privacy.

Slide 10:

(Michael)

So, to that end, what role does the U.S. Department of Education play in protecting student privacy? Most importantly, we administer and enforce a number of federal laws governing the privacy of student information, including two laws that we'll be talking about today in the context of using online educational services: the Family Educational Rights and Privacy Act (or FERPA, for short), and the Protection of Pupil Rights Amendment, or PPRA. But, administering and enforcing these laws is not all that we do to protect student privacy (though it does keep our Family Policy Compliance Office very busy). We also work to raise awareness throughout the education community of the privacy risks and challenges involved when collecting and using student data. We provide both general and targeted technical assistance, through PTAC, on privacy and security issues to schools, districts, and states, and we are active in promoting a number of privacy and security best practices that we encourage education stakeholders to adopt.

Slide 12:

(Michael)

Put simply, FERPA guarantees parents access to the information contained in their children's education records, and protects those records from unauthorized disclosure without the parents' consent. More specifically, FERPA gives parents the right to access and seek to amend their children's education records. The law protects any personally identifiable information (or PII) from those education records from unauthorized disclosure, and it requires written consent from the parent before sharing PII with third parties…unless an exception applies.

Slide 13:

(Michael)

There are a number of these exceptions to FERPA's written consent requirement – and those of you who have sat through any of our prior webinars are undoubtedly familiar with some of them. For today's discussion, we're going to focus exclusively on two of these exceptions: the Directory Information exception and the school official exception. But, as I said, there are a number of other exceptions to this consent requirement, and we'll have a link to the PTAC website at the end of the presentation if you want to find out more information about any of them. So, Baron, can you tell us about these two exceptions to FERPA's consent requirement?

Slide 14:

(Baron)

We know students don't attend school anonymously, therefore FERPA allows schools to release certain information without consent. Some examples include, name, address, email address, photographs, degrees, and awards received (such as valedictorian). Keep in mind that much of this information could be PII and just because you *can* do it, doesn't mean it's a best practice. In addition, remember that schools must provide the list of what they consider directory information in its annual notification to parents and that parents can opt out of that information being shared.

Slide 15:

(Baron)

Some common uses of this exception are yearbooks, student directories, and concert programs. Remember that parents have the right to opt out!

Slide 16:

(Baron)

The school official exception is generally the exception that allows those involved in the education of students to be able to deliver education services needed to the student. When involving a third party provider, or TPP, it's important the following caveats are met: One, it has to be a service or function that the school/district would otherwise use its own employees. For example, this could be student information system services or dashboards provided by a vendor. Two, the use of the data by that TPP is under the direct control of that provider with regard to the use and maintenance of those education records. Three, the use of the data aligns with the annual notification sent to parents on what constitutes a school official with a legitimate education interest. And finally, the data is not used for unauthorized purposes.

Slide 18:

(Michael)

Though the PPRA has been around for many years, its most notable changes—for the purposes of today's discussion—were introduced when it was amended as part of the No Child Left Behind Act of 2001. While the law is mostly known for its provisions dealing with surveys in elementary and secondary schools (the so-called "Sex, Drugs, and Rock and Roll" provisions) it also includes limitations on the use of personal information collected from students for marketing purposes.

Slide 19:

(Baron)

We're going to move on to some commonly asked questions now. First up:

Is student information used in online educational services protected by FERPA?

Slide 20:

(Michael)

As much as I wish I could give a definitive answer to that question, and as much as I appreciate those on Twitter who recently poked fun at us for saying it in the guidance document, the real answer to that question is "It depends." Some data used in online educational services is absolutely protected by FERPA—say, for instance, the student profile information (like name, grade, and email address) that a school enters into an online system to create students' user accounts. When that information is taken from education records (like the school's Student Information System) then FERPA would absolutely be implicated. But, there are many different types of online services, and even more types of data—much of which probably isn't protected by FERPA. Take, for instance, an online portal that students use to watch tutorials or complete interactive exercises without logging in or using individual accounts. In these cases, no PII is involved, so FERPA would not apply. In the end, schools and districts will typically need to evaluate the use of online educational services on a case-by-case basis, to determine if FERPA-protected information is implicated.

Slide 21:

(Baron)

Question two, what does FERPA require if PII from students' education records is disclosed to a provider?

Slide 22:

(Michael)

Well, the most straightforward approach would be to have parents provide written consent for their children's information to be disclosed to the service provider. But, as anyone who has ever tried to collect field trip permission slips can attest, this is often not an efficient process, and may be unworkable for essential services central to the education process. Without written parental consent, disclosure of PII from education records can only occur under one of FERPA's exceptions to the consent requirement. In the case of online educational services, this will most likely be done under one of the two exceptions we discussed earlier. The Directory Information exception is an easy way to disclose student information to create student accounts—but only if all of the data elements that will be disclosed are properly designated as directory information in the school's or district's annual notice. Also, using the Directory Information exception may be problematic in those cases where parents have elected to "opt out" of directory information. It is often unfeasible for a school to maintain two separate systems for the same function—an online one for the majority of students, and a separate, paper-based one for those students whose parents have opted out of Directory Information.

Slide 23:

(Baron)

Question three, under FERPA and PPRA, are providers limited in what they can do with the student information they collect or receive?

Slide 24:

(Michael)

Again, I'll have to say, "It depends." In this case, it depends on how the information was collected or disclosed. If the PII was disclosed under the Directory Information exception, then typically there would be no other limitations on using the data for other purposes. If the information was disclosed under the School Official exception, on the other hand, then the PII may only be used for the specific purpose for which it was disclosed. Third Party Providers are prohibited from selling or sharing the PII, or using it for any other purpose except as directed by the school or district, and as permitted by FERPA. But, whether or not FERPA-protected information is implicated, whenever personal information is collected from a student the PPRA may also apply. So the PPRA's restrictions on marketing may apply even when there are no other legal protections on the data.

Slide 25:

(Michael)

We want to stress, though, that FERPA and the PPRA represent minimum legal requirements. They are the floor, not the ceiling when it comes to protecting students' privacy. Schools and Districts can, and often should, consider placing additional limitations on what online service providers can do with student information by inserting those provisions into their agreements with the service providers.

Slide 26:

(Baron)

Michael, I hear the word metadata thrown around quite a bit. What is it? And are there restrictions on what providers can do with metadata about students' interactions with their services?

Slide 27:

(Michael)

So, you're right. Metadata has been used a lot in the news recently, and many of those who use the term have not done a very good job explaining what it actually means. Put simply, metadata are pieces of information that provide meaning and context to other data being collected or used. For example, if we were interested in tracking a student's performance on a particular online activity (or, as is more often the case, trying to find patterns in how a large number of students perform on a specific activity) we would want to know how the students did on the activity (the data), but that performance information would have a whole lot more meaning and analytical use if you also knew the date and time the student performed the activity, the number of attempts they made, how long their mouse hovered over the answer button (which is an indicator of indecision), or whether they changed their answer

before submitting it. All of these other pieces of contextual information, collectively known as "metadata," are tremendously useful for education technology developers in building and enhancing the underlying algorithms used in personalized learning and other similar technologies. Metadata that have been stripped of all their direct identifiers and other indirect identifying information are *not* protected under FERPA, because at that point they are no longer considered to be PII. I'll make the important caveat, however, that when you're looking to de-identify metadata it is important to consider that, depending on the context, school name or other geographic information can be indirect identifiers in student data. People often forget that point. Assuming it's done properly, de-identified metadata can be used by providers for any number of other purposes, unless prohibited by other laws, or by more restrictive data use provisions in the provider's agreement with the school or district.

Slide 28:

(Baron)

There are other laws to consider such as COPPA which applies to commercial websites and online services directed to children under age 13. This law is administered by the Federal Trade Commission. Please see the link for more information.

Slide 29:

(Baron)

Now we will walk you through several best practices on protecting student privacy. The first, which we just discussed, is that it's critical to be aware of other relevant laws, such as COPPA, that may apply. You should also be aware of your local, state, or tribal laws. In fact, many states and local entities have pending or passed laws regarding the protection of student personally identifiable information.

Slide 30:

(Michael)

Administrators will also want to be aware of which online educational services are currently in use in your school or district. The first step in protecting student data is knowing what information is being collected or shared, by whom, and for what purposes. And you can't even begin to answer these questions until you know what services are being used across your organization.

Slide 31:

(Baron)

It's important that your organization has policies and procedures consistent with state, local, and federal law to evaluate and approve proposed education services. For instance, you may have a policy that requires that any new software must be reviewed by legal, IT, and management prior to being implemented in a classroom setting.

Slide 32:

So, Baron, on that subject, can individual teachers sign up for free (or "freemium") education services to use in their classrooms?

Slide 33:

(Baron)

Many say, "nothing is free." And in many cases, from Facebook to your grocery's frequent shopper card, identifiable information or marketing information is your "payment" for the service. It's important to remember that FERPA has requirements, which we discussed earlier, that you must adhere with when using these types of software/apps. Also, remember that many free apps can introduce security vulnerabilities into your school networks. Most importantly, we consider it a best practice to have regular trainings with staff around your policies regarding the use of software, downloads, and "free services."

Slide 34:

(Michael)

Good to know. Getting back to our list of best practices to consider, though FERPA does not expressly require that schools or districts use a written contract or legal agreement when disclosing information under the school official exception, we strongly recommend that schools and districts do so, whenever possible. Not only do these agreements help with the "direct control" requirements we discussed earlier, but they also serve to clarify the use restrictions and other legal requirements that the provider is expected to meet.

Slide 35:

(Baron)

Transparency is critical when it comes to communicating with parents and students on how data is being used, who it's being shared with, and for what purpose. We highly recommend that school districts inform parents of how children's data is being used, what information is being shared, and for what purpose in a public forum such as a website.

Slide 36:

(Michael)

And lastly, while there are many circumstances where obtaining parental consent is just not feasible, hence FERPA's exceptions, there are many other circumstances where obtaining parental consent is the best way to go. Going the consent route is a great way to increase transparency about your school or district's data use, and many districts are doing it to communicate with parents about what their kids

are doing online. So, we understand that it's not always an option, but we do recommend it whenever possible.

Slide 37:

(Baron)

So, Michael. What provisions should be in a school's or district's contract with a provider?

Slide 38:

Good question. Again, FERPA does not expressly require that schools or districts use a contract or written agreement with a third party provider, but for all the reasons we've discussed, it is absolutely a best practice to do so, and there are a number of provisions that we recommend including in those agreements when you develop them.

For starters, we recommend including data security and data stewardship provisions. Make it clear whether the data being collected belongs to the school or the provider, and describe each party's responsibility in the event of a data breach. You can even establish minimum security controls that the provider should use, and allow for auditing of their compliance with those controls. We also recommend clearly specifying what information the provider will be collecting through their service (logs, cookies, tracking pixels, whatever it may be). It's hard to assess and mitigate the privacy risk of a technology if you don't even know what information it's collecting! Be sure to define the specific purposes for which the provider may use student information, and legally bind them only to those approved uses. How long will the provider hold on to the data in identifiable form? Will they be permitted to share it with any other party? When the contract ends, how should they handle destroying the data? All of these are important terms to consider laying out in a written agreement. We recommend specifying whether the school, district, or parent will be permitted to access the data in the system, and if so, the process for obtaining access. This is particularly important if the provider will be creating or maintaining education records for the school, as FERPA's access rights would then come into play. We recommend establishing how long the agreement will be in force, and what the terms are for modifying, amending, or terminating the agreement. This is particularly important for reasons we'll talk about a little later. And lastly, we recommend considering whether there should (or should not) be any provisions wherein the school or district indemnifies the provider, or vice versa, particularly as it relates to the school or district's potential liabilities resulting from failure to comply with federal, state, or tribal law.

Slide 39:

(Baron)

Michael, what about online educational services that use "click-wrap" agreements instead of traditional contracts?

Slide 40:

(Michael)

So, as we mentioned before, “Click Wrap” agreements are a particular form of legal agreement between a service provider and the user of that service. They are essentially a compilation of “take-it-or-leave-it” legal provisions established by the provider to which the user agrees by clicking “accept.” Not accepting these provisions means not using the service, plain and simple.

Well, these click-wrap agreements pose a challenge for the use of online educational services because they muddy the waters a bit about how the various legal requirements and best practices will be met. Consequently, we recommend that schools or districts take extra caution and apply extra scrutiny to these agreements before accepting them and using the services.

First, schools and districts should be sure to check the amendment provisions. Many click-wrap agreements allow the provider to unilaterally change the terms of the agreement without notice to the user. Given the FERPA school official’s exception requirement to maintain “direct control” over the use of student information, we recommend that schools and districts exercise caution when agreeing to any terms of service that allows for amendment without notice. And if you do enter into them, we recommend reviewing the agreements regularly to determine if any provisions have changed.

We recommend printing (or saving) any terms of service agreement that you accept. Remember, these are legally binding agreements between the vendor and the school or district – you should be sure to keep a copy for future reference.

And lastly, because these click-wrap agreements are legally binding documents between the provider and the school or district, and because they are so easy to agree to with one quick click of a mouse button, we recommend that districts (or schools) establish policies that specify who has authority to accept terms of service agreements, and what they should be reviewing these agreements for prior to accepting them.

Slide 44:

(Baron)

Thank you for attending today’s webinar. We appreciate your attention and look forward to hearing more from you regarding your thoughts/comments on this document. Please send your comments to privacyta@ed.gov.