FTC Workshop: Student Privacy and Ed Tech
December 1, 2017
Segment 1: Introduction, Opening Remarks, Panel 1
Transcript

KRISTIN COHEN: We're going to go ahead and get started, so please take your seats if you can. So, good morning. We're excited to see so many of you here today. On behalf of my colleagues here at the Federal Trade Commission as well as our colleagues at the Department of Education who are co-hosting this workshop, we'd like to welcome you to the Student Privacy and Ed Tech Workshop. My name is Kristin Cohen. I am an attorney in the Division of Privacy and Identity Protection at the FTC. My co-organizers for today's event from the FTC are Peder Magee and Laura Hosken, and from the Department of Education, Kathleen Styles, who is their Chief Privacy Officer, Michael Hawes, who is the Director of Student Privacy Policy, and Tracey Kumare, a privacy policy analyst.

Before we get started with our program, I just need to go over a couple of administrative details. Please silence any mobile phones. If you need to use them during the conference, please just be respectful of the panelists and the other audience members. Please be aware if you need to leave the building at any point, you do have to go back through security. So keep that in mind. The restrooms are right outside the auditorium. The cafeteria is open until 3:00, and you don't have to go back through security if you use the cafeteria, so I recommend that. But please do remember that there is no food and drink allowed in the auditorium other than water.

Most of you got an FTC event lanyard security badge. We do reuse those. So, please turn them in at the end of the day. If an emergency occurs where we have to leave the auditorium but stay in the building, just follow the instructions on the building PA. And if we do have to leave the building, please exit out of the 7th Street exit and cross over, down 7th, across E Street, and that's where we'll congregate. If you notice any suspicious activity, please alert building security. And please be advised that this event will be photographed and is being webcast and recorded. By participating in this event, you're agreeing that your image and anything you say or submit may be posted on ftc.gov or any of our social media sites.

We are happy to welcome those watching via the webcast. That webcast will be available on our workshop web page after the event. So if any of your colleagues aren't here today and would like to watch any of this or you have to miss any part of it, you can watch it at a later time. We will be leaving time for audience questions during each of the panels today. Question cards are available in the hallway immediately outside of the conference room on the materials table. If you have a question, just write it down, raise your hand, someone will come along and collect those questions, and we will try to get through as many of them as we can.

We are also live tweeting this on Twitter, at #edtechFTC. So if you would like to follow along, that'd be great. And if you want to ask a question via Twitter, just tweet @FTC and that hashtag, #edtechFTC. And lastly, I just want to thank our panelists for coming today, as well as Crystal Peters and Bruce Jennings, who have helped us here at the FTC to put this conference together, as well as our paralegal support from Olivia Berry, Patrick Curtin, David Aguayo, John Ade, Christine Barker, and Courtney Brown. We also want to thank our Division of Consumer and

Business Ed for helping put our conference materials together and our Office of Public Affairs, Juliana Gruenwald Henderson and Nicole Jones, who have helped us out a lot in this process. Now it is my honor to welcome the acting director of the Bureau of Consumer Protection at the FTC, Tom Pahl, to give opening remarks.

[APPLAUSE]

THOMAS B. PAUL: Great. Thank you, Kristin. And good morning, everyone. I'm losing my voice a bit, so I'll try to speak up. But if my voice tends to decrease a bit, please try to listen attentively and I'll soldier on through my remarks today.

Welcome to the joint FTC/Department of Education workshop on student privacy and ed tech. I want to begin by thanking all of the workshop participants for taking the time from their important duties to share their expertise and for all of you for coming here today to join us. I'd also like to thank the staff of both agencies for their hard work in putting this day together. In particular, I'd like to thank Peder Magee, Kristin Cohen, Mark Eichorn, and Maneesha Mithal, from our Bureau of Consumer Protection, and Laura Hosken, from our Bureau of Economics. I'd also like to thank Kathleen Styles, Michael Hawes, and Tracey Kumare from the Department of Education. We're really looking forward to our discussion here today.

As we all know, computers and other technologies are ubiquitous in the contemporary classroom. And ed tech is here to stay. We want to make ed tech as beneficial as possible for educators, parents, and students alike. We want to ensure that student privacy is necessarily part of that calculus, and that's why we're here today.

One theme of today's event is how well 20th century laws and approaches have kept up with 21st century technologies. We'll talk about the Family Educational Rights and Privacy Act, or FERPA, which protects the privacy of student educational records. That law was passed in 1974, well before the advent of the internet.

Think about what was going on in 1974 in terms of technological developments. The pocket calculator became available in stores for the first time. Supermarkets were installing the first barcode scanners. And Toshiba was introducing the first floppy disk drives. In schools, we were still being taught that diamonds were the hardest substance, the Great Wall of China was the only structure on Earth that could be visible from outer space, and that Pluto was actually a planet.

Note to some of the other old-timers in the audience, none of these things are actually true anymore. We'll also talk about the Children's Online Privacy Protection Act rule, or COPPA rule, which the FTC first issued in 1999. That year, there was one computer in the classroom for every nine students. In 2000, 20% of schools still did not have broadband internet access. If you mentioned ed tech back in that time period, people probably would have looked around the room for a guy named Ed. Now, less than a generation later, nearly half of students have access to their own school-provided internet-connected device, and online curriculum is becoming increasingly the norm.

With more and more of our children's schoolwork online, it is imperative that federal laws and regulations protecting students' privacy keeps pace. At the same time, we need to ensure that schools have the flexibility to do what they are there to do-- educate our children. Today's workshop is at the intersection of COPPA, FERPA, and ed tech. In my opening remarks, I'd like to begin by providing some background on COPPA and FERPA, next I'll highlight some of the key issues that we hope to discuss today, and finally I'll preview the day's agenda.

Well, the two statutes that we're going to be discussing today are COPPA and FERPA. COPPA applies to the commercial online collection of information from kids, when they are surfing the internet from their PC at home, through a mobile app when they're on the go, or at school using some sort of ed tech program. The FTC first issued its COPPA rule in 1999 and updated the rule in 2013 to address new trends in social media, mobile app usage, behavioral advertising, and new types of personal information children were sharing online, such as photos and video. Since 1999, the FTC has brought 26 law enforcement actions against companies, alleging violations of COPPA. And we have obtained more than $9.5 million in civil penalties from these firms.

During the 1999 rulemaking process, the commission received comments raising concerns about requiring parental consent for online information in the classroom. The commenters explained that this could be very disruptive to schools, especially when only one or two students did not receive parental permission. In response, the FTC decided that schools could act as intermediaries between online operators and parents, and when an operator received consent from a school, it could presume that the school had obtained the parents' consent.

It would be great if I could say today problem solved. However, in 1999, the use of internet in schools was minimal. In contrast, many of today's students carry an internet-connected device to each class. That device holds their textbooks, allows them to submit assignments electronically, provides mobile apps to practice their reading and math skills, and provides a platform for teachers to communicate with their students about assignments and questions. These students are working with multiple ed tech providers and sharing large amounts of personal information.

So, in addition to the practical challenges of obtaining parental consent that we heard about at the commission back in 1999, we now also hear from parents and privacy advocates concerns about the scope of information collection happening in schools, sometimes with parents knowing little about the extent of the information collection. In particular, parents and advocates raise concerns about secondary uses of information collected from their kids in the school environment.

For example, we have heard from parents worried that ed tech providers will use the information they collect in the school context to market non-educational products to students. We need to examine how our guidance on COPPA has held up in light of these developments.

The second statute that we're going to discuss today is FERPA. FERPA generally prohibits educational agencies and institutions from disclosing student educational records without a parent's prior written consent. As with the FTC, that Department of Education has worked to ensure that FERPA keeps pace with changes in the classroom. For example, in 2014 the Department issued guidance explaining that a prohibition on disclosure of personal information from student records without first getting parental consent does not preclude schools from sharing that information with ed tech providers.

However, to do so, the school must follow the requirements of the school official exception to FERPA's written consent requirement. In other words, the school can generally provide student data to an ed tech provider if the provider is performing a function the school's employees otherwise would perform and that several other additional criteria are met, including that the provider is appropriately restricting reuse and disclosure of that information.

So, why are we here today? Well, both agencies have issued guidance and tried to keep up and balance student privacy concerns with the need for schools to have flexibility and take advantage of new educational technologies in the classroom, yet many tough questions remain. Let me highlight three questions that we will be discussing today. First, under COPPA, even as schools can stand in the shoes of parents and consent to the collection of information from kids, what right should parents have to access and delete their children's information?

On the one hand, COPPA gives parents a clear right to access and deletion. On the other hand, schools often use ed tech products that commercial entities provide to administer homeworks, grades, and test scores. This raises the issue of whether and how parents should be able to delete classwork information and grades.

Not students, however-- I want to make the point that we at the FTC are opposed to students being able to go in and change their grades electronically. If students want to do that, they're going to have to do it like I did back in the day, and do it the old-fashioned way. But anyway, if parents have rights to access and deletion, how can they exercise the rights in a way that won't interfere with the school's role in educating students?

A second issue that I think is going to be predominant in our discussions today involves consent to information collection for children that is limited to educational purposes. There may be some questions around the parameters. What is an educational purpose? For example, should use of kids' information to improve school-related products and services be permissible? In other words, if a school contracts with an ed tech vendor to use a reading app in the classroom, can the provider then turn around and use the personal information collected from students to improve that app? How about to create a different reading app? How about to develop an unrelated educational app, such as a math app?

Third issue that we are likely to focus on today is questions about the intersections between COPPA and FERPA. For example, while they both apply to personal information about students, their definition of what constitutes personal information differ. Moreover, FERPA is primarily directed at schools, while COPPA is primarily directed at ed tech vendors.

With the continued proliferation of new ed tech products, new uses, and new questions about the intersection of COPPA and FERPA, both the FTC and the Department of Education believe further discussion and perhaps additional guidance is warranted. We hope that a robust discussion among those with a variety of viewpoints to identify where the law may be unclear or inconsistent, in or between these two regulatory schemes, can be had today. Today's discussion should provide a roadmap for us in terms of potential next steps at the agencies.

This workshop provides an opportunity for stakeholders, including students, parents, and ed tech providers to discuss how best to protect our students' privacy, while also giving schools flexibility to use new tools in the classroom. We'll kick off the day today with a series of background presentations to set the stage for our panel discussions. We'll start by hearing from Heather Whitaker, who works in the Department of Education's Office of Educational Technology. She'll provide background about educational technology being used in schools today.

We'll follow that with a brief presentation by the FTC's Peder Magee on current COPPA guidance around consent in the classroom setting, and by Michael Hawes, the Director of Student Privacy Policy, Department of Education, who will provide us with the basics of FERPA and ed tech. Finally, we'll hear from Amelia Vance, Education Policy Counsel at the Future of Privacy Forum, who tells us how new state laws have been addressing student privacy.

Following these presentations, we will hear from a series of panels. The first panel will focus on the perspective of schools, both large and small. We'll hear about how schools are using ed tech and the practical challenges they face in working with different types of products and services. We'll also hear about how one school district in Colorado addressed the privacy concerns of parents in its district, and from that parent who raised those concerns and built a parent-student privacy coalition.

The next panel will highlight the questions and concerns around student privacy and ed tech and how COPPA and FERPA apply in this context. Finally, we will end the day with a panel considering next steps, including possibly releasing additional guidance on this important topic. My colleague, Kathleen Styles from the Department of Education will provide closing remarks.

So I'm going to turn the podium over to Heather Whitaker, the Special Assistant in the Department of Education's Office of Educational Technology, who will start us off with an overview of how ed tech is being used in the classroom. Thank you very much.

[APPLAUSE]

HEATHER A. WHITAKER: Well good morning. My name is Heather Whitaker. I am a special assistant in the Office of Educational Technology at the US Department of Education. And for the past 13 years, I have been a teacher, a middle school assistant principal, and most recently an elementary school principal in a one-to-one school district for the last six years.

The Office of Educational Technology is an ed tech policy shop in the Office of the Secretary. And we bridge the department and the ed tech community. We work with states, local districts, and institutions to develop educational technology policy and establish a vision for how technology can be used to transform teaching and learning and make everywhere all the time learning possible for all learners.

Technology and education has exploded over the past several years. It has really been a powerful tool for transforming learning. Technology can help and affirm and advance relationships between educators and students, reinvent our approaches to learning and collaborating, shrink longstanding equity and accessibility gaps, and adapt learning experiences to meet the needs of all learners. We are on an exponential pace of technology change. Many new technologies continue to converge, from artificial technologies, IA, virtual reality, and augmented reality to technologies that offer hope of curing diseases.

The rapid advancement in technologies are changing the landscape of learning today, more than ever before, how students learn, how teachers learn, and how to empower and engage all of our students. Just to give you a perspective on this, the newest generations are called Generation Z, which they are approximately five years old to 19 years old, and then Generation Alpha, which are five years old and yet to be born. These generations have not known the world without technology or the internet, and they are very comfortable with the use of technology. They have grown up using Google to search, apps to perform daily tasks, and social media to communicate. They totally embrace the fast pace of the world of evolving technology products.

So let's take a quick look at a timeline. I know Thomas just did a brief explanation of some things that have changed rapidly, and the same thing with the tech world. The search engine was developed in 1997; the first iPod, 2001; the first iPhone only 10 years ago, 2007; the iPad, 2010, which is in a majority of our schools today; 2012, the Google Glasses; 2014, Apple Watches, that many of you probably own; virtual reality, 2014; hover boards, of course-- everyone wants one of those for Christmas already-- 2015; touchable 3D holograms, 2015; Amazon Echo Dots, with Alexa that talk to you in your home.

And American scientists are using gene editing techniques called CRISPRs to customize T cells to turn them into cancer-killing genes. Tesla rolled out a driverless car. And doctors are using technology to put small computer chips on the brain to restore movement from spinal cord injuries, which is amazing. So there's more and more things that are coming out each day that are just things we can't even imagine or think about.

Schools are not just using computers alone to teach and learn with. They are using just about every type of device and hardware-- smartphones, tablets, laptops, voice-activated devices, and more. And software is the same way. They use Twitter, Snapchat, coding apps, avatar programs to teach or new, upcoming teachers, movie-making products, pictures, editing software, and this goes on and on as well. They are using all of this to create personalized learning plans that engage each student. Teachers are blending together multiple teaching philosophies to create critical thinkers. More schools have added STEM programs for their elementary-aged children, all of this being made possible by the advancements in educational technology.

These continuing advancements in technology have allowed students to learn in the manner and setting that best suits them, whether it be a public, home school, private, charter, online, magnet, or many of the other options given to students and parents.

The National Education Technology Plan, the NETP, is our flagship educational technology policy document for the United States. In order for the NETP vision of everywhere, all the time learning to be realized, there needs to be access to online tools and resources, needed to be reliable and present in schools, as well as outside of schools. In order to provide students with the education they need to thrive in a globally connected world, we must find ways to fund, acquire, and maintain the infrastructure that will make connectivity a reality for each and every teacher and every student in every learning environment.

We must be very mindful and intentional of the security and protection of our children in this ever-changing space of technology. But we must not stifle this valuable learning process. That being said, digital citizenship has never been more important. With increase to access of one-to-one devices, educators and parents need to make sure they have knowledge and access to curriculum and programs to support teaching good digital citizenship skills. We can put blocking and security features in place. But for that to work, we must also teach our children how to be safe digital citizens to protect themselves now and later in life.

Just to give you an idea of just how far we have come in connecting everyone everywhere, in 2013, just 30% of our schools met the 100 kilobytes per second per student goal. Last data released by Education Superhighway show 94% of our schools are now connected at that rate, and that's phenomenal. We still have a long way to go, though. The great news is that we have 94, but we still have 6.5 million students left to connect. And to meet future demands, the typical school district will need to grow bandwidth at least 2.6 times and ensure all over Wi-Fi to support all the digital learning that is going to be taking place.

The NETP also discusses the use of technology-enabled assessments and support for the learning and teaching of communicating evidence of the learning process taking place. This is accomplished by providing data and immediate feedback to teachers, administrators, families, and most importantly to the learners themselves. New software and devices are allowing the feedback to be immediate to all stakeholders. These assessments can be embedded within the digital learning activities to reduce interruptions in the learning time. Personalized and evidence-based learning has never been so feasible and accessible to all students. For more information and for examples on this, you can access the NETP at tech.ed.gov.

In education, we talk a lot about personalized learning and how important it is. But what is personalized learning? Many people confuse it or use it interchangeably with other terms such as active learning, blended learning, competency-based learning, differentiated learning, and individualized learning. Although these terms have similar and overlapping-- in at least one area, with personalized learning-- they have different meanings. So we're going to talk about those for just a second.

Adaptive learning is technology is used to assign human and digital resources to learners, based on their unique needs-- so, like, social, emotional needs, or special physical needs that they have. Individualized learning is the pace of learning. It is adjusted to meet the needs of the individual student. So adaptive learning is actually a good example of providing individualized learning and distance education as well. Differentiated learning, the approach to learning, is adjusted to meet the needs of the individual student. So students may be grouped in areas of their interest, and that helps them differentiate learning. And competency-based learning-- learners advance through a learning pathway based on their ability of demonstrating competency, so mastering skills at their own speed.

In the NETP, the US Department of Education gives its shared definition of personalized learning, referring to instruction in which the pace of learning and instruction approach are optimized for the need of each learner. Learning objectives, instructional approaches, and instructional content and its sequencing may all vary based on the learners' need. In addition, learning activities are made available that are meaningful and relevant to each learner and driven by their interests and often self-initiated.

There are many potential benefits to personalized learning. Here's just a few of them. When a pace of learning is adjusted for each learner, all learners have the time needed to demonstrate mastery. When learning is supported by technology, learners can receive more frequent and immediate feedback through formative assessments, quizzes, and checks for understanding, with results provided to teachers and learners in real time. With the right tools, learning gaps that impede progress can be identified more quickly in allowing learners to close that learning gap.

When teachers can use technology to identify or modify existing resources more easily, teachers can then build stronger and deeper relationships with each learner and provide more resources in dealing with their actual specific challenges. This can promote a greater sense of belonging among the students by demonstrating that there are adults that care about if they are thriving or not.

In closing, we need to understand that technology is now as important as textbooks used to be when we were growing up. Students can no longer be successful learning the important skills needed to be successful in this global 21st century community without technology. Thank you. And if you have any questions, you can contact us. And you can also tweet that at #edtechFTC. Thank you.

[APPLAUSE]

PEDER MAGEE: Thanks, Heather. Good morning, everyone. My name is Peder Magee. I'm an attorney at the FTC. I'm going to provide a short overview of the Children's Online Privacy Protection Act, how it works, who's covered, and generally how it applies in the school/educational context. I see we've got some of the big experts in the audience, so I apologize in advance if some of this is a little rudimentary.

All right, a little background on COPPA. Congress passed COPPA in 1998 in order to give parents more control over the online collection of data from their kids. As all parents know, children don't always make the best choices. And there was a concern at the time that as more and more kids were accessing the internet, going online, there needed to be some additional safeguards in place to protect them.

Congress directed the FTC along with the states to enforce the law, which we do through the Commission's COPPA rule. The Commission issued that in 1999. The rule fleshes out some of the requirements set forth in the statute and provides more specificity.

The Commission periodically undertakes a review of the COPPA rule in order to ensure that it's keeping pace with changes in technology and new business models. In 2012, after a robust rulemaking process that included a couple of rounds of public comment, the FTC amended the rule. Among other things, the amendments added to the list of covered personal information, it strengthened the security requirements, and it also expanded coverage to certain new third parties.

Now, the basic requirement, absent one of the rules exceptions, COPPA requires covered operators to provide notice and obtain parental consent before collecting personal information from kids under 13 years of age-- or in the case of this slide, an infant. Although we focus on the notice and consent aspects often, COPPA also has important additional requirements, including that operators have reasonable data security and that they provide parents the ability to access and delete their kids' collected information, among other things.

So let me walk through the various elements of when COPPA applies. First, COPPA is the Children's Online Privacy Protection Act, so it only applies to online data collection. Think, anything you can access through your browser or anything that lets you interact on your device, mobile apps, VoIP services, and increasingly connected toys and other IoT, or Internet of Things, products that are intended for children.

Next, COPPA does not apply to everyone collecting information online. Instead, COPPA basically divides the world into two categories. The first, sites and services that are directed to kids, and then sites and services intended for a general audience. If you fall into the child-directed category, you have to assume that everyone who comes to your site or that uses your app is a child. The Commission considers a variety of factors in determining whether something is child-directed. These include things like the use of animated characters, or child-oriented activities, also the actual audience demographics. Those factors are set forth in the Commission's COPPA rule.

Now, if you're a general audience site or service, you only have to comply with COPPA if you have actual knowledge that you're collecting personal information from kids under 13. In addition, if you're a general audience site and you have actual knowledge that you're collecting from users of a third party child-directed site-- so for instance, if you're a plug-in and you're installed on a child-directed site, if you have actual knowledge that you're on that site and you're collecting from users of that site, you can also incur COPPA liability.

Keep in mind that COPPA is triggered by the collection of personal information from a child. The rule sets out the list of covered types of information. It can be obvious things like a home address or a person's full name. But it can also be things like-- it includes things such as a persistent identifier in a cookie. And as I mentioned, the Commission expanded this list in 2012. One of the new categories covers photos, videos, and audio captured from a child.

OK. So, if you're covered, you've got to provide notice, and that includes two things-- having a privacy policy that sets out your information practices, as well as a specific direct notice spelling out things like the data you collect, whether you're going to share it, that parental consent is necessary. Next, you have to obtain verifiable parental consent to collect the data. There are a number of ways to do that. The rule sets out some examples, but operators are free to come up with their own VPC method, so long as it's reasonably calculated in light of available technology to ensure that the person providing consent is the parent. Also, you have to comply with the other COPPA requirements as well, things like providing access, having data security, retention limitations.

All right, so that's how COPPA applies in general. But one of the reasons we are here today is that there are some important wrinkles on how COPPA applies in the school/educational context. As you're going to hear, while FERPA covers schools, COPPA looks to the ed tech vendors that operate websites and services that are actually collecting personal information from kids. Schools themselves typically are not commercial operators of websites or services, and the FTC does not have jurisdiction over non-profits like public schools.

That being said, schools are often asked to play a role with respect to COPPA consent. Going back to 1999, there was an interest in allowing technologies into the classroom. And during the Commission's rulemaking process, the FTC sought to take into account concerns that requiring parental consent for online collection in the class would interfere with educational activities.

So in an effort to accommodate the use of ed tech in schools, the Commission took the position that the rule does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process. It also does not preclude schools from serving as the parents' agent in the process.

And what that means is that where an operator is authorized by a school to collect personal information from children, the operator can presume that the school's authorization is based on the school having obtained consent. In other words, the operator doesn't have to get consent from the parent.

The operator is not off the hook, though. If the school is providing consent, the operator has to provide the school with a notice it would otherwise have provided to the parents. In addition, in the Commission's COPPA rule FAQs, the Commission has further indicated that school's ability to consent is limited to the educational context and that an operator may not use the collected information for some other commercial purpose outside of the educational purpose. And then finally, as a best practice, the Commission has recommended that consent come from the school or district rather than from an individual teacher.

So that's COPPA in the general and in the school context in a nutshell. I just want to tee up some of the questions that we're going to be getting into today to sort of whet your appetite for our upcoming panels. We're going to be talking about how schools should provide COPPA consent, process ed tech providers should use appropriate limitations on the use of data when the school provides consent, and then how the other COPPA requirements play out in this context.

Finally, I want to mention that the FTC has some great materials on our website about COPPA, including a set of FAQs as well as a six-step guide to complying with the COPPA rule. And with that, I'll turn it over to my colleague from the Department of Ed to walk us through FERPA. Thank you.

[APPLAUSE]

MICHAEL B. HAWES: Good morning. So, I was given 10 minutes to cover FERPA here. So, those of you who understand FERPA in the audience realize how much of a challenge that is. So I'm going to stress the 101 portion of today's discussion. This is really just the teaser trailer, if you will, of how FERPA applies in the ed tech context.

So, Peder discussed how COPPA applies and who COPPA applies to. And COPPA applies to operators of these services. FERPA applies to any educational agency or institution that receives funds under any program administered by the US Secretary of Education. So here we're talking about requirements that schools, school districts, and so on, must meet.

The Family Educational Rights and Privacy Act was passed in 1974. And it gives parents and eligible students the right to access and to seek to amend their children's education records. An eligible student in this context is a student who is enrolled at a post-secondary institution or who has turned 18.

FERPA also protects any personally identifiable information from a student's education record from unauthorized disclosure, and it requires that written consent be provided by the parents or the eligible student before disclosure is made, unless an exception applies. Now, there are two terms there that require a little bit of definition. Personally identifiable information under FERPA is a fairly broad definition. It includes your obvious direct identifiers, those data elements that have a one-to-one relationship to a child-- like a name, student ID number, social security number, et cetera. It includes indirect identifiers-- those pieces of information that may have a many-to-one relationship to a student, like place of birth, date of birth, various demographic information.

But FERPA also includes a third category of information in its definition of PII, and that's any other information that either by itself or in combination with other information is linked or linkable to a specific student and that would allow a reasonable person in the school community to re-identify the student with any reasonable certainty. So essentially what this third catch-all category means is that there is no defined list of PII data elements under FERPA. A variety of types of information can be considered PII, depending on the context and what other information is being collected.

The other term that requires definition in this context is education record. And under the law, an education record is any record that is directly related to the student and that is maintained either by or on behalf of an educational agency or institution. And as we talk in a little bit, that's going to have implications for the information collected by ed tech providers participating in classroom activities.

So, the big question when discussing how FERPA applies in the ed tech space is, is the student information that's used in online educational services protected by FERPA? And those of you who are familiar with FERPA in the audience, and there are many of you, you know that the answer to just about any FERPA question is always "it depends." And it's going to depend a lot on the context and the information you're discussing.

And the answer to this question is no different. Some of the information that's used or collected by online ed tech providers and online educational services are absolutely protected by FERPA. Other data may not be, and it's going to depend on how the information is being collected, whether it's linked specifically to a specific student, and a variety of other factors. But much of the information that is used in online educational services in the classroom would have some FERPA protections attached to it. We recommend the schools and districts evaluate the use of their online educational services on a case-by-case basis to determine whether the information implicated is covered under FERPA or not.

So, I mentioned before that FERPA requires that you have written parental consent before you disclose any FERPA protected information, any PII from a student's education record, to a third party. But there are some exceptions to that consent requirement. And two of those exceptions are particularly relevant in the online educational services context. Those two exceptions are the directory information exception and the school official exception, and we'll cover each of these in a little more detail in a moment.

I do want to stress, these are only two of the exceptions to the consent requirement under the law. There are a number of others. And you can go to the regulations or you can go to our website to get information on the other exceptions to this consent requirement.

So, the directory information exception-- so, the directory information exception exists because students don't attend schools anonymously. There are a variety of normal day-to-day activities that occur in schools that routinely require some amount of student information to be disclosed in the broader community-- think school yearbooks or telephone directories, concert programs. There's quite a variety of activities where some information about students is routinely disclosed.

So, the directory information exception allows schools and school districts to disclose certain information that's deemed less harmful without consent. But in order to do so, schools and districts must designate the various data elements that they consider to be directory information and provide notice to parents about which elements they do consider to be directory information. And they have to give parents the opportunity to opt out of disclosures under the directory information exception. So a parent has the rights to say, you know, you've designated these elements as directory information, I would prefer you not disclose those for my child. And then schools are not able to then disclose those pieces of information for that student.

The other exception that's particularly important in the context of education technology is the school official exception. And this exception allows schools and districts to disclose PII from students education records without parental consent to certain third parties, provided that that third party is performing a service or function that the school district would otherwise use their own employees to perform. Also, the third party must be under the direct control of the school or district with regard to how they're using and maintaining the PII from education records. And at our panel this afternoon, we'll be discussing more what direct control means.

Also, the third party can only then use the PII from education records in a manner that's consistent with how the school has defined school official with legitimate educational interest in their annual notice to students-- sorry, annual notice to parents of their rights under FERPA. And the third party is not allowed to disclose or to use the educational information for any unauthorized purpose. There we go.

So, with this in mind, when we're thinking about how schools disclose information as part of their use of online educational technology, there's three ways that student information can be provided to online service providers. The first would be by obtaining written parental consent. The second could be through the directory information exception. And the third could be through the school official exception. Each of these methods have their own limitations and their own requirements.

Key here, consents, for anyone who has ever been a teacher, you know that it can be often difficult to obtain parental consent for even worthwhile activities. Consent is a great option-- it is the most transparent, it is the most privacy protective-- but can be problematic when you're talking about required school services. If you are using a student information system and all students must be in it and you're requiring parental consent to do so, well then you have some challenges, because under FERPA you cannot require a parent to waive their rights as a condition of attendance in public school. And then how do you deal with students whose parents have opted out of the use of a required technology? So consent can be problematic in some contexts.

Directory information, similarly, can be problematic, because only those data elements that have been properly designated as directory information can be disclosed to a third party. And any other information that's being collected or used as part of the school activity that is then linked to that directory information calls into question whether this is still directory information or not. You could be essentially linking more FERPA-protected information to directory information, and then that exception would not apply. The third, with the school official exception, as I mentioned, this allows the disclosure of PII without consent, but you then must meet those requirements of the school official exception, including being under the direct control of the school or district.

So, are providers that receive PII from education records limited in what they can do with the student information that they collect or receive? Well, again, the answer is, it depends. And that's going to depend on which of those exceptions or which method they received the PII under. If the PII was disclosed using written consent from the parent, then the provider would only be limited by the provisions that are included in that consent statement. If the PII was disclosed under the directory information exception, generally there would be no limitations on what could be done with that directory information, though there are exceptions to that.

Lastly, if the PII is disclosed under the school official exception, which is by far the most common method under which education technology receives student information, then again they must meet the requirements of the school official exception, and they can only use the information they receive for the specific purposes for which it was disclosed. And the providers can't sell or share the PII or use it for any other purpose except as directed by the school and in compliance with FERPA.

So, that was a very brief overview of how FERPA applies in the online educational technology context. There's much more information on this topic available through our 2014 guidance, "Protecting Student Privacy While Using Online Educational Services." That's available at our website, studentprivacy.ed.gov.

If you have questions relating to this, we have a privacy technical assistance center that has a variety of other resources relating to this and other student privacy topics. And we have a help desk for specific questions that you might have. So with that, I'm going to turn things over to Amelia Vance to talk about state privacy laws, and thank you very much.

[APPLAUSE]

AMELIA VANCE: Good morning. And thanks to all of you for coming out for student privacy. It's always great to see so many people interested in this topic. Hopefully I can progress the slides safely. Yes!

So, before I dig into the state laws, I think it's really important to set the context of why we've had over 600 bills introduced in 49 states, specifically on student privacy, since 2013. A lot of this is-- it's really a broad landscape of privacy concerns. Part of it is the general confusion over what technology actually means. We use amorphous terms like "the cloud" to describe where we're storing information and how we're protecting it. And I've been in a room with a bunch of tech experts and asked, can you describe the cloud to anyone in a sentence? And I think two people raised their hand.

At the end of the day, it's really an offsite server you can access remotely. And we don't make it easy for people to understand the technology and what we're using. There's a lot of jargon here, and it creates a lot of questions for parents, for teachers, for administrators about exactly what is happening with the technology in our classroom.

We also have a very different scope and type of student data that schools collect. We've always had records. But now we have, with a lot of the great ed tech that Heather laid out in the classroom, more types of data being collected. And it's a lot bigger than it used to be. There's the potential for much more information to be collected.

And so there are a lot of concerns around, are we collecting the right things? Are people collecting data just for the sake of collecting data? And how are we using it? What is the value to the individual student? How are we showing that value to parents and to educators and to administrators in the use of ed tech?

There's also a lot of concern across pretty much every area of the spectrum about who is collecting and accessing student data and education records. No Child Left Behind brought in a new era of data that was being sent to the federal government for extremely great purposes. We wouldn't have the study, for example, that came out in the past year showing that there are disproportionate suspension rates of minority students and that minority students are routinely not referred to AP classes without this information. But the fact that there's more information going to state and federal governments than before can be concerning.

You also have many more third parties involved in all of this, which can be positive. They can engage students through ed tech in ways they've never been engaged before, can help students who need accommodations that haven't been able to adequately get the education that they deserve. But where does this information go? And we've been very bad about, again, explaining the value and explaining exactly why certain parties are receiving certain information.

There's a general concern, of course, about how it's being used-- again, back to this value proposition. And then there's the overall privacy beyond data issues that we've always had. When do we have free speech in schools, and can students say what they want to? When can schools look at social media accounts and punish students for what they are saying online? When can these devices that we're providing to individual students be searched by the school or be accessed? Or when is that information and thought process that could be shown through a search history or something else-- when is that private to the student?

And so this has led to 124 laws since 2013 passing in 40 states. As I mentioned, 49 states have introduced bills. We've had at least 100 bills introduced every single year, starting in 2014. Again, specifically on student privacy-- this doesn't encompass the wider spectrum of bills that are introduced on things like data breach notification that also sometimes impact schools. This has been a massive legal shift, and it has been very hard for schools, states, ed tech providers to keep up and understand what their obligations are.

A couple of things I want to mention about some of the trends here that I'm going to be going over fairly quickly. We mentioned the definitions of personal information in COPPA and FERPA. This has been to some point made null by a lot of these state laws. Most state laws views personal information as anything that is personally identifiable about the student, which means that whether or not it's in an education record, that information is protected under those state laws.

You also have nonprofit ed tech providers covered. So the fact that COPPA does not cover nonprofit ed tech providers doesn't really matter in those particular states. We've had a couple of divisions that sometimes overlap in the state law trends. We've seen governance focused laws and more prohibitive laws. The prohibitive laws have focused much more on, how do we ban the things that we're afraid of? How do we make sure that that information we think is inappropriate doesn't go to third parties or the government? How do we restrict what type of information is collected in the first place?

On the governance side-- and these are mostly focused at schools and state education agencies-- it's about, do you have someone who can answer people's questions? Do you have a policy in place? These are the things that must be in your policy. These are the transparency measures, for better or worse, that you must put in place which sometimes provide actual transparency to parents and sometimes are more like in a 120-page PDF. So there have been a really wide variety in the laws that we've seen.

The other difference in state laws is who is covered. Prior to 2013, you had a decent number of states that already had student privacy laws, but many of them just repeated the requirements under FERPA. Under the new laws, as I mentioned, we got much more detailed about what schools and state education agencies were required to do.

And then there was a new element. You suddenly had several states that were introducing and passing laws directly aimed at ed tech providers. I wanted to include this very quickly. I run this website Ferpa Sherpa, the education privacy resource center, and we have a full list of all of these state laws and who they target that you can look at and see if your state has actually passed a law. And I believe these slides are available after as well.

The laws aimed at vendors, which I want to focus on because they're most pertinent to the conversation today, are really based on California's law SOPIPA. I'll go through exactly what SOPIPA consists of, but it is by far the most common type of law that is passed in student privacy over the past couple of years, with 19 states so far passing pretty similar versions of SOPIPA. SOPIPA applies to operators of a website-- and I'm using the California definition here, so notice this may vary from state to state-- of a website online service or online or mobile application when their product is for K-12 school purposes and was also designed and marketed for K-12 purposes. It protects personal information in any media or format that is provided to the operator by the student or parent for school purposes, by the school district or LEA, or is gathered by the operator through the operation of their service, and is descriptive of a student or otherwise identifies a student.

Under SOPIPA, and this pretty much carries across all of the versions, an operator cannot target advertising. They cannot create a profile, except for K-12 school purposes. They are not allowed to sell a student's information or disclose covered information. And they must implement and maintain reasonable security procedures and practices-- a fairly common term in tech law because you don't want to include a very specific security standard that will be outdated tomorrow-- and then they must delete information when asked by the local education agency.

Really quickly, I want to go through what we've seen in the aftermath of these state laws. We've seen a lot of unintended consequences. Because, as I mentioned, some of the laws have been more fear-based, there's been a tendency by legislatures to perhaps overreact and not think carefully and talk to all of the various stakeholders who need information and who deal with this data and technology every day. Perhaps the best example of this is Louisiana, which passed an incredibly restrictive law in 2014. This law prohibited any personal information being disclosed unless parents opted in to sharing that information.

The law was also written extremely vaguely. And you had districts-- because if you accidentally gave away information, you could go to jail or you could be fined as an individual teacher or administrator. And so you had schools that were afraid to have yearbooks, to announce football player names, to hang student artwork in the hallway, and most unfortunately, to refer students to the state scholarship fund. You had teachers who had to go to students' homes, and even then you could not get enough parents to opt in, whether it was by choice or just the fact that they weren't there, and it caused utter havoc. The law was mostly repealed when it came to those district restrictions the following year, because it just wasn't tenable.

You've also seen similar difficulties in other states. Some states have set an end size of 10, or basically saying that you can't disclose information unless you have more than 10 students in a subgroup. Unfortunately, again, they hadn't quite checked with their districts. And 56% of high school graduation rates in Oklahoma could not be disclosed to the public because of this policy.

Another great example is New Hampshire, which did not allow for video recordings in the classroom unless you got the consent of the school board, all parents, all students, and the educator themselves, which sounds pretty reasonable-- onerous, but reasonable-- but it greatly restricted the ability of special education students who needed those recordings as part of their individualized education plans.

We also have a lot of interesting trends. As I mentioned, governance and the mandate to actually document policies at the district and state level and to think about transparency has been incredibly beneficial, where when parents now go to districts or states, there's much more likely to be someone who can actually answer their questions, which is incredibly important.

There have been some states-- this is growing year by year in the legislation that's been introduced, Utah, in particular, has been phenomenal at this-- that have focused on training. Unfortunately, though, as of last year, only 18 of the 500 laws introduced mention training. Fewer than that provided funding. So there's a whole lot of state laws that have no requirements that teachers be trained in these incredibly detailed requirements to protect student information, and no funding to actually carry out those mandates.

You also have requirements to audit, to make sure that the laws are followed and that districts are doing what the law says. You have a mix of opt in or out requirements, which tends to work very well when it's for non-specific education-- or not required educational services. So things that are being used sort of like a textbook in the classroom maybe is not subject to an opt out but a supplemental math game can be.

You've seen some device and social media privacy bills. And then finally, you've seen a variety of penalties, mostly in the form of fines. But we have seen a couple of states, like Louisiana, that have jail time if you accidentally release information, or much more commonly, if there is a purposeful and planned release of information violating those student privacy laws.

I am more than happy to talk more about state laws with anyone at the break, or if you want to contact me. Thank you so much for listening.

[APPLAUSE]

PEDER MAGEE: Thanks, Amelia. We're going to take a break until 10:25. And then our next panel will explore perspectives of several schools. And we're going to hear the viewpoints of a parent who raised privacy concerns with her particular school district. Refreshments are available for purchase in the cafeteria, which is just down the hall, if you take a left when you go out the doors. And just a reminder, please don't bring food or drink back into the auditorium. Thanks.