FTC Workshop: Student Privacy and Ed Tech
December 1, 2017
Segment 3: Panel 3
Transcript

PEDER MAGEE: OK, I think we're going to get started on panel three, if people want to take their seats. So Panel 3 is called Student Privacy Issues and Challenges. And we have a great group here.

To my left, Linnette Attai, who's president of PlayWell LLC. Next to her is Dan Crowley, the trust and safety manager at Quizlet. Then there's Bill Fitzgerald, technologist from Common Sense Media, Priscilla Regan, professor at George Mason University, and Melissa Tebbenkamp, who's the director of instructional technology for Raytown Quality Schools, Missouri. I'm Peder Magee, and with me is Michael, who will be co-moderating.

Great. So as I said, the panel is about privacy issues and challenges. And what I'd like to do is kick things off by directing the first question to Priscilla. Priscilla, COPPA, and even more so, FERPA were enacted in a very different world than what we have today, technologically speaking at least. Could you talk about what you see as today's privacy issues or concerns with respect to ed tech, sort of a bigger picture?

PRISCILLA M. REGAN: OK, thank you, Peder. I've been writing and thinking about privacy policy since the late '70s. So there's a little bit of a context here in terms of the complexity of privacy.

So this is a multifaceted value. And we often use it to encompass a number of different concerns. And I think this is true in the ed tech environment as well. But it's important that we sort of separate out and identify the separate concerns so that we can ensure that policy is really addressing all of those concerns.

So I'm going to go through them quickly. We can talk more about them later. There's basically, I think, six concerns regarding ed tech that fall under the privacy rubric. And the first is the classic information privacy concern. And this is COPPA and FERPA both are sort of designed in that environment regarding the collection, the use, the retention, the disclosure of personal information.

And I think this gets challenged in the ed tech environment in a couple of ways. There's sort of more quantity of information that's being collected. And there's often a different quality-- qualitative information that's being collected. So more pieces are kind of being picked up. And so this gets more complicated, because you've also got parental concerns that come into play, and the education relationship is mandatory and not voluntary.

The second privacy concern is that, generally, or often, when people talk about privacy, they're also talking about the ability to remain anonymous or to have what is sometimes called practical obscurity. And I think this is also somewhat challenged here, because with the collection of so much data and the retention of so much data, it's difficult to anonymize, or it becomes more difficult to anonymize that data.

And it's easy to re-identify students. And this is where we get into sort of the algorithmic searches, the use of artificial intelligence, the fact that personally identifiable information is sort of a less meaningful concept. So that is something that's also wrapped up in here, that ability to remain anonymous or for a student to have some kind of practical obscurity.

The third is the surveillance and tracking that takes place, that's in effect, facilitated by ed tech. Here with sort of online testing and different teaching programs, the programs are monitoring and analyzing what the students are doing at that time. And things like how long it might take to read a page, the patterns and the ways in which students are reading and responding, which gives some indication, then, of the students' thought processes. And also, when and where they are working, who else may be working on similar things at similar times, especially when these programs are being used both in school and at home or in other environments. So those are concerns of surveillance and tracking.

A fourth concern has to do with the autonomy. The autonomy of the student, the kind of individual will, creativity that we want students to exercise. So if information is being fed into predictive analytic programs that are determining students' patterns and strengths and weaknesses and personalized learning, all of which has advantages, but it can also track students or narrow students too quickly, and foreclose options that students may have developed on their own.

And they may be, if they're aware of this more probably in the middle schools and high schools, they may self-censor what they're doing. And at any of the ages from K through 12, the fact that they may be directed in a certain way may limit their creativity. So that autonomy aspect of privacy, I think, is also an important one.

And the fifth one is sort of traditional due process. Sometimes when we're talking about privacy, we're really talking about fairness and treating people equally, that individuals should be treated fairly and equally, and they shouldn't be discriminated against. This is obviously critical in the ed tech and the education environment generally, because of the importance of education to equal opportunity.

And here, with the kind of algorithmic analysis that takes place, it can sometimes make identification of bias and discrimination difficult to identify, and then hard to reverse. So I think there's a concern that prejudging students, that could lead to discrimination. And then finally is when people talk about privacy at certain points, people have talked about a property interest in information and who owns the information.

Generally speaking, does the individual own the information or does a third party own the information? In the school environment, generally, the school records are owned by the school. But clearly, the FERPA in particular ensures parental rights. And I think here then we really get into, as has been discussed in the earlier panels, the importance of the contracts and the way contracts are written.

PEDER MAGEE: Great, thank you. Does anyone want to comment on that? Any other thoughts? Well, maybe I can direct one to Bill. Could you talk about Common Sense Media's privacy initiative, maybe some of the insights you've gained through evaluating different privacy policies from tech vendors?

BILL FITZGERALD: Yeah sure. Just also want to start by thanking the people at the FTC and the DOE who put this together. This is actually just-- we need to have more events like this where we can actually all talk. And just thank you for getting us all here in the room so we can have these conversations.

So as part of my day job, I am part of a small team where we basically spend our days reading privacy policies. It's fun. You should come join us. But yeah, we do this all the time.

And we start to see a range of patterns across the board. And sometimes we actually see a lot of evidence of really good practice and really good thought that goes into these. Like there are some vendors who have actually studiously listed out the data they collect. They've listed out the third parties they use. They've listed out what information each third party gets. They've listed out limits that are placed on these third parties.

And they do this, like, it's accurate. And I verify that it's accurate, because I run all these site who are intercepting proxy, and you can actually track it one to one. So we see things like that, which are great. And that is-- that's a change. Like two years ago, I didn't see that.

On the other end of the spectrum, we also see vendors who have policies that have no relationship to their apps or to their websites. And there's a real disconnect between what the terms state and what the service does. And often, when we point this out, the response is, well, yes, but our app only does this, so you shouldn't judge us by what we say in our terms.

And it's one of those moments where, unfortunately, I would love to-- in ed tech, nobody wakes up and they rub their hands together and it's like, ah, how can I profit off of kids today? That's not the space. There are other industries where people can do that more effectively and they generally go there.

But when we look at the gap between when somebody policies have drifted from what the app does, we have to believe the policies. We can't take somebody on their word as to their intent, because their policies actually stake out what they can do. And this is something that we still see on a pretty regular basis.

And I think-- I mean, we see it too much in 2017. This is something that should have changed. So one of the things that would be a great shift to see would be a shift to having vendors actually describe what their app does now, not what their business plan states their app might do in the future. Because as we analyze policies and as we make evaluations based on those policies, we have to believe your words. And that's what-- I think the more we can actually look at policies as a statement of intent and as a statement of business plan, we can start to get a clearer sense of how these services will support students and learners.

PEDER MAGEE: Thanks. Bill, your comment that you filed in advance of the workshop notes that there's been both under and over compliance by educators, as well as the vendors in their approach to complying with COPPA and FERPA. And I wonder if you could talk a little bit about how you've seen that play out.

BILL FITZGERALD: Well, and also I'd like to highlight, too, you that Ariel Fox Johnson did a lot of the legwork on this. So I don't want to take credit for work that is also reflective of her input. What was kind of behind that is-- and this has been alluded to in some of the states that have passed transparency laws. Like the response has been a 120-page PDF to show how transparent you are.

And that's what I call over compliance, because you actually have some really specific needs that have been laid out. And rather than actually meet those needs, you throw up an obfuscation field, and you do it in the least accessible format possible, the PDF, which is where information goes to die. And so yeah, you're complying with the law, but that's what I call over compliance, because yeah, legally you're off the hook, but practically you haven't advanced the bar.

PEDER MAGEE: Great. Linnette, I'm wondering if you have seen any of that type of thing with any of the work that you've done, this idea of over and under compliance with the two statutes?

LINNETTE ATTAI: Yes, and I think it's really important to level set us here. We've heard a lot so far this morning from both panels. And I think Bill touched on something very important, which is that not all vendors are alike. We need to remember that not all school districts are alike, not all and parent groups are alike.

We have different perspectives. Some are better at these things than others. Some are more sophisticated in their knowledge, more mature in their governance systems than others. I agree with Bill that I don't see anyone trying to do something malicious here. I see lack of information, lack of knowledge, lack of fluency.

So when I see-- frankly, when I see some vendors being I think what Bill would describe as being over compliant, I think it's important to also look at the ecosystem that we're operating in when vendors will get an RFP from a school district that will ask 100 questions about their security practices. And we're pretty confident, because of the nature of the questions being asked, the school district doesn't know what the answers would tell them.

We get asked in-- vendors get asked in contracts to comply with just about every law ever written about anything. I've seen vendors be asked to comply with an entire state's education code, when about three paragraphs of it applies to the vendor. And the entire code is about 300 pages about how to build a board, rules about when kids can go to the bathroom in classrooms. And that's not a joke.

So I think when you see that instinct to over comply is almost this instinct to, like, I don't know what information you're asking for, so I'm going to give you everything I possibly can think of that might be useful to you. And perhaps that's misguided, but I think there's also a natural reaction to try to say, I don't know what it is, school, that you need in order to be comfortable with this tool.

So here's everything I know and I'm just going to give that to you. And I appreciate that that's not a helpful format. And often, not helpful information. But I just want to paint the picture of the ecosystem in which that exists. In addition with state laws, we heard Amelia speak this morning, 600 bills written, we have upwards of 120 state student data privacy laws across 40 states. Very poor definitions, contradictions within each law, almost no guidance from any state on implementation of the law or defining what they meant when they said no data mining, and didn't define those terms, and didn't define personal information.

So I think to a certain extent, vendors are trying to figure it out, just as districts are trying to figure it out and parents are trying to figure it out. And the ecosystem just hasn't evolved yet to a place where there is a solid answer. But I do think, also, we have companies that are trying to be transparent in different ways, not just in their privacy policy, but also in trying to build very consumer friendly website pages where they talk about their privacy practices, the data they collect in as plain language as possible.

Privacy policies are hard to read sometimes. And we get that. But there are also some legal requirements, some things that have to be in privacy policies. There's class action litigation that we need to be mindful of. So what I'm seeing is a lot of companies really trying to strip the jargon out of those policies, but also sometimes when they can't do that fully, to build up a more parent friendly, school friendly place on their site to be more transparent about it.

PEDER MAGEE: Great Melissa, have you seen that sort of thing, where perhaps the vendors are overcompensating or unsure of what sort of information they need to disclose, and have, then, as a result, just disclosed everything?

MELISSA TEBBENKAMP: Absolutely. There are numerous versions of privacy policies in terms of service that are out there. And you can definitely tell the companies who really have vetted the process and have used appropriate counsel to know where their space is in education and really what we need to know. And then those who are just throwing everything in there, because frankly, some are afraid and some are just taking the last one that they read and trying to make it theirs as well.

And so that's where that conversation comes in with that vendor, because we're going to partner with them. And if we're going to bring them into our schools, we need that partnership. And so we need them to understand what services we need from them and we need to understand what they're providing to us and making sure that we're both on the same page. And then rewrite those to meet our needs.

PEDER MAGEE: Great. OK, I think that sets the stage pretty well. I'd like to shift a little bit and maybe drill down somewhat on some of the COPPA implications here. And as we discussed earlier this morning, we talked about how COPPA has taken the approach that schools can provide consent in the place of parents. And I'm wondering, and I'll throw this out to anyone who wants to take it, how that's played out. Maybe talk about some of the challenges this approach raises from the school perspective, and also from the ed tech vendor perspective.

MELISSA TEBBENKAMP: I'll start with a school perspective. We collect-- in Raytown, we have parents sign every year saying that they know that we're using sites. And we have a link to the sites that we're using that collect data, and the data that they're collecting.

But we also go further than that. And if a site explicitly says you need parental consent, we know they're doing something other than what we intend for them to do with their data. And we have that conversation to clarify that. And at that point, we just don't use the site.

And that's a decision that we've made, because we were protecting our data. But we also know that it's impossible for us to get parental consent for every single one of our students. And then what does that do to the classroom?

And so we urge our partners, our vendors, our service providers to really work with us to, one, protect the data, but at that point, we just won't use that site. And that's the choice that we've made. Other districts choose to go on and go that path. With the larger student population and a higher transient rate, it's not manageable for us to be able to use sites that require that additional parental consent. And so if we can act on behalf of the parent and bring that in as an educational agent, then we will. But if not, then we just avoid those.

PEDER MAGEE: Dan, maybe you'd like you give your perspective on that?

DAN CROWLEY: Yeah, so from the vendor perspective, there's a lot of complexity the moment you want to have school providing consent under COPPA. You have the 120 different state laws. You have FERPA, you have COPPA, if you're working internationally, you have international privacy regulations. There's a lot of just additional complexity.

And then you're getting with state and local policies, you're trying to verify that a district is, in fact, who they say they are and they can provide that content under COPPA. And so you're trying to do all of the right things and make sure that the school has all the right information, the parents have all the right information. And that's really-- the administrative overhead of that is pretty intense, especially when you add on the additional layer of that intermediary between yourself as the vendor and then the parent.

So I'll say, at Quizlet, we don't work through the district. We want our to be involved. We want our parents to know when their child is using Quizlet. And so we always require parental consent. And that's a choice that we've made. And I think that that works for us.

We're a supplemental study tool. We're not an assessment platform. We're not kind of that direct to district grading provider or LMS. We're that supplemental study tool that was started because a 16-year-old wanted to create an app for himself and his friends to study. And that's how we were founded.

And that's always been at the core of our mission. And so it's always been about the students. And we think parents need to be involved in that process. And so we think, for us, that's been the right decision. But then also, that complicates things, because you have a lot of districts who have their own policy. They want to be involved in there too.

And so I think it works better in the supplemental, voluntary model that Quizlet can exist in. But there are huge administrative burdens when you have these more kind of classic enterprise, B2B providers where it's a grade. It's a disciplinary record. It's attendance.

And so I think that's where you get those operational burdens on generally pretty small companies. I mean, there are obviously-- there are some big ones that are out there. But a lot of us aren't that big. Quizlet's, I think, around 65 people right now. That's generally the size of the company that you're working with.

And we're out here trying to do our best to give teachers and students tools to improve their education, to help them do what they do best. Let teachers teach as effectively as they want with the best tools that are available to them. And their professional opinion can help them help a student, to help a student learn how they can study, how they can grow, how they can pass their math class, how they can pass their social studies class.

We take that obligation seriously. These are children and students whose lives we're helping to change. And we come into work every day incredibly mindful of the trust that is placed in us as a vendor. And that's why we don't have a privacy team, we have a trust team.

PEDER MAGEE: Thank you. It looks like, Priscilla, you wanted to weight in, and then we'll go to Bill.

PRISCILLA M. REGAN: Yeah, I think a clarification Dan, does Quizlet then-- is the teacher recommending Quizlet or is it just are you dealing directly with parents? Is it used in the classroom as well or just at home?

BILL FITZGERALD: So it is-- we know it's used in both. We've always been-- when we started it was just about students. And what we've seen is that as students use this and students started bringing-- students brought it into the classroom. And it was the students, they were creating their own study material.

And the teacher would see this change in the student and ask, well, what's going on with you? And they would say, oh, Quizlet. Then the teacher comes and says, well, maybe I can use this tool to help more of my students.

PRISCILLA M. REGAN: And at that point, then the school district gets in, or the school gets involved.

PEDER MAGEE: So we don't have any--

PRISCILLA M. REGAN: Any involve-- OK, you bypass that completely.

BILL FITZGERALD: We don't have any customized contracts with a district. I think is important to note that if a teacher wants to create a study set for their use of students, we don't require a login to access that content. The teacher could, but content on Quizlet is available without providing any personal information to us whatsoever.

PRISCILLA M. REGAN: OK.

PEDER MAGEE: And Bill, did you want to--

BILL FITZGERALD: Yeah, one of the things that we see with consent and that we see from actually reading a lot of terms is that a lot of vendors will just explicitly say, it's the teacher responsibility to do this. And this kind of brings up two things. I mean, first is-- the elephant in the room in some cases with consent is the idea that consent actually protects privacy. Consent means that you're actually just agreeing to what the terms say. So you've actually then agreed that whatever happens in the terms can actually happen with your kid.

So again, the consent there is going to be as meaningful or as unmeaningful as the terms. But the other piece on this is that because it's deferred to the teacher, the teacher is often creating-- the teacher's actually making a determination that they may or may not be able to make that an application has a strictly educational purpose. And that's actually very difficult.

If that is on the teacher, then the teacher is essentially on the hook for that. And I don't think many people-- I don't really think anybody wants to explore that, because the implications for that are really going to be problematic for a lot of people. I think we need to explore that, because that's actually one of the big-- like there's how consent was framed, what it should do, and then there's how it's practiced. And again, the practice has drifted radically from the intent of how it was framed.

LINNETTE ATTAI: And I think there are obviously a wide variety of technologies, right? There's the enterprise technologies, which are usually contracted with the district. Then there is this whole ecosystem of apps and websites. I think 500, 700 were numbers that were thrown out earlier that may be used across a district that teachers may just bring into the classroom.

However, I would disagree that we're not talking about that. I actually work with a number of districts on what is essentially this governance challenge of teachers bringing apps and websites into the classroom, clicking to agree to terms of use, not really understanding what they are agreeing to, but just kind of moving past the barriers in order to get that technology into the classroom. And it is, it's an organizational governance challenge for districts, and one that a variety of districts I've worked with have had a lot of success.

I think Allen spoke pretty eloquently to this earlier to-- and it's a very common pressure that CTOs and CIOs in districts have when teachers say, stop telling me that I have to have my technology vetted. You're in the way of innovation. But there are really simple things that we do to kind of ease that-- essentially, change management process and get teachers to start appreciating the value of vetting. One is to remind them that by clicking on a terms of use, you are binding your organization to a contract, which you may or may not have the authority to do.

And so often what I encourage districts to do is to say, OK teachers, here's where we're going to start. Every time you bring an app or a website into the classroom, I want you to copy and paste those terms of use and the privacy policy. I want to date it and sign it like its contract and just file it with me. I'm not going to stand in your way. But you sign that.

And that, in and of itself, puts a lot of teachers back on their heels and says, oh wait, could you just do that first for me? I also have districts that will then put a small checklist, maybe five questions. Does it say what happens to the data when we're no longer using this? Does it tell you what data they're collecting, who's getting the consents? Just check those boxes, maybe highlight in the contract where you saw that for me, then sign it and date it.

And what you're doing, really, is starting to change the culture in the organization, because we're not training teachers on privacy. We're not trying the ecosystem on privacy. But we have to start talking about it. And sometimes we can't just rip off the Band-Aid and say, OK, starting today you're all going to have your technology vetted without bottlenecking the entire system. So we have to think of creative ways to introduce change, just as we do in any organization.

PEDER MAGEE: All right, thanks. Well, we talked a bit about the consents. And I get the message. And I think we heard this earlier that there needs to be some training and some information. And one of COPPA's hallmarks is that, in addition to consent, it requires that operators give parents notice about the information practices, what they're collecting, what they're doing with it, things of that nature.

So when we've said that the school can give the consent on behalf of the parents, my question is, what are the challenges or issues associated with the vendor then giving the notice to the school? And maybe, Melissa, what's been your experience in terms of the notice that the vendors get to the school, and is it enough? Does it put you in a position to educate the parents about what's going on? If you could talk about that a bit.

MELISSA TEBBENKAMP: So we handle adoption centralized for our students, or for all of our curriculum. And so all of those resources come through my office and a colleague of mine, and we vet those. And if at that point that we are going to use a resource that tracks student data, then that comes to me for contract negotiation.

And we don't adopt those standard terms of service and privacy policy, because of the notification pieces of there. And instead, we write our own that work and explicitly just state what types of classification of data that they're collecting. And I require vendors to give us that information in the form of a data inventory.

Because I do believe that we need to know what data they're collecting and how that's being collected. And also, what data we're sharing with them. So it's a two-way road. They need to know what data we're sending to them. And we're very careful to only send them the data that they need to perform the job that we're asking them to do for us.

So they might want date of birth, but to them it doesn't matter. Or to us it doesn't matter if they have that information, so we just won't send that. So we negotiate what data is being transmitted to them and then what data that they're collecting. And we handle that outside of the normal terms of service and privacy policy.

I know not all districts have the capacity to do that. And that's where I think it goes back to having our partners that are really great about posting that. There's many of them out there that are posting exactly what's being collected.

I have a few that, honestly, I give them a call, I'm like, oh my goodness, your privacy policy is amazing. It has everything I need in it. That is great. We just need to change one term of where we're going to go into arbitration, because I want it in my state. And so this is the one term we're changing and then we're good to go. And so there's a lot of great partners out there that are doing it well, and then there are some that aren't. And so we just take those individually.

PEDER MAGEE: I think that that raises an issue that's interesting. It sounds like, from your perspect-- you're in a fairly good position where you're able to perhaps push back on terms of service and things. And we did touch-- we touched upon it in the earlier panel that not all schools are in that position. And I'm wondering if anyone has thoughts on how that plays out for perhaps smaller schools or schools with less resources.

MELISSA TEBBENKAMP: If I can start with that. It starts with the leadership. I have a great leadership team in our district, and they all buy in to data privacy. That's something that we hang our hat on and we take very important. I often say that schools really focus on the physical security of their students, and we should also think about the digital security of them as well.

And so there is a whole leadership framework. We've bailed on a very critical system three weeks before school started because they weren't able to meet our data governance needs. And we were OK with doing that. Did I have panicked voices saying we need this? Absolutely. But instead, we found another resource to fit that need because that company wasn't willing to partner with us.

It starts with the leadership and then it goes from there. And if you have that leadership, then you can do that. In small districts, believe it or not, I also hear that we don't have the power to push back on a company. But we're all customers, and if they want our business, and if we are unified and that, then we'll be-- you know, they're not making money without us. And so if we're unified in the approach of what we need with data governance, then we can make a difference no matter how big or small.

Raytown's not huge. We're 9,000 students. It's not like we're a 250,000 student district. And we're still able to push back and get what we need for our kids.

PEDER MAGEE: Bill, I think you wanted to interject.

BILL FITZGERALD: Yeah, I mean one of the things you said is something I've heard repeated many times, which is people, particularly from smaller districts, will often say they just can't get their calls returned from vendors. But unlike your situation, they don't have the support to actually not use the vendor, so they end up getting steamrolled.

And there's a lot-- I mean, there's a lot of resentment towards some vendors out there who are not responsive to school needs. And the ability to actually have-- actually to say no and revamp a system is something that a lot of districts won't do. But this is also something-- also as part of my work at Common Sense, I staff a consortium of about 140 districts nationwide.

And the work that Steve is doing is part of the STPC. Districts are actually starting to band together to have a collective voice, which makes it easier for districts to get results that they need from these conversations. It also makes it easier, actually, for the vendors to listen, because they can have one conversation instead of 100 conversations. But I think in looking at some creative ways to both unify district voice and streamline vendor response to reasonable and repeated requests, we can actually start to make improvements here.

DAN CROWLEY: I'll jump in from the vendor side, but I think that's true. I mean, we're trying to build products that work. And so that means we do need to listen. And if we're not building a product that works, then that's something we want to change.

And so we don't think of privacy just as our policy or our terms. It's beyond that. It's a whole program. There's transparency that has to go into there. You want to be responsible in disclosing-- we do disclose who our third party providers are. That's part of it.

And then there's features within the product that let teachers and districts meet their own obligations and their own policies. And that's something that, when we hear about, those are things that we can then start to work to build towards. We're not going to know every district's policies. Like we simply can do that. But when we find them, then we have an opportunity to meet those needs. And those are needs that largely we do want to meet.

LINNETTE ATTAI: And I think that there are resources out there for districts of all sizes. It doesn't need to be an us versus them scenario. In fact, I have the luxury of working with vendors, with schools and districts, but also I'm the project director for CoSN Privacy Initiative and have been able to, at some scale, go out and work with districts and educate them on their own governance responsibilities, vetting technologies, contracting with vendors, negotiating.

I was in Connecticut earlier in November speaking to almost half the districts in the state around this very challenge, and working with them, collaborating with them, giving them tools and tips, giving them the view from the other side of the table. What does it mean when my vendor gives me red lines? What do I do? How do I push back?

And there is a culture within school organizations that it just didn't grow up as businesses to understand how to do that business transaction. And so there are a lot of organizations like CoSN that are providing free resources and educating districts at scale around these very things to help them get smarter, get more adept, and build partnerships with vendors, instead of feeling as if they have to kind of go up against-- vendors are not the big bad wolf and schools are not all frail beings. But you've got to find that middle ground, find that partnership, and be open and transparent and build a collaboration.

PEDER MAGEE: OK, I want to shift a little bit the focus. And I think this is one of the leading issues, at least in the COPPA world in this space, and that's the-- it's the question of how ed tech vendors can use data when the school is providing consent. FERPA requires that the vendor only use the information for the purposes for which it was disclosed, and that it be under the control of the school. And the FTC has taken the approach that if the school is giving consent, the use has to be for educational purposes and no other commercial purpose.

And while that sounds pretty straightforward, I think it raises a lot of issues on where you draw that line. And I'd like to just open it up to the panel on your thoughts and what sort of practical challenges that might present. Maybe, Priscilla, you--

PRISCILLA M. REGAN: I get to go first.

PEDER MAGEE: You can start first.

PRISCILLA M. REGAN: Well, I think that it's clearly hard, as Melissa was saying, to get consent from parents. I think that having the school districts give consent makes sense, but then I think the inventory, along the lines that you were talking about, that the schools have given consent, but then there's clear notice to the parents. And that notice has to be organized in a way that makes sense.

The sort of common sense approach here is one that I think is key, because you're really-- I mean, the key-- you're trying to develop trust here. The word partnership has been used by a number of the panelists. And I think that in order to do that, you've got to communicate and you've got to build that trust. That trust doesn't just sort of occur overnight.

So the communication between and among the vendors, the school districts, and the parents is really key. I mean, we don't want to get into, quite yet, the purposes of giving consent, just a general topic of consent?

PEDER MAGEE: Well, yes, but I would like to hear thoughts on how you make the cut on this is for an educational purpose and no other purpose. I mean, can there be-- if the vendor's collecting information and they're improving their product, or they're improving a related educational product. Thoughts on where that line is.

PRISCILLA M. REGAN: I'm going to be somebody who's going to draw that line rather narrowly. That educational purpose is the educational purpose for which it was intended, which is basically the classroom use and the students' learning. The product development piece I see as a commercial, sort of secondary use. And that there, you would need to get parents' consent. And I think when you get parents' consent, it shouldn't be incentivized in some way, that if you give consent, then you'll get this benefit.

And it has to be, we're doing a lot of nudging in society nowadays. The vendor shouldn't be nudging the parents to give consent to the product development. And I think in some of the comments and some of the arguments have been made, the analogy has been drawn to the textbooks, that textbook publishers, many of whom also entered the ed tech field, have always used the feedback in order to improve the product.

And you want the product to be improved. There, the feedback came from the teachers. How did that product work in terms of learning? And I don't have a problem with teachers giving feedback on the product, how the product is working. But I don't think the companies should be using the data in that way to do their analysis. I realize I may well be in the minority on that.

PEDER MAGEE: Well, let's find out from the rest of the panelists. What are other thoughts on where that line is?

BILL FITZGERALD: Well, I mean there are a few assumptions embedded in this that I think also need to get drawn out. I mean, one of the things-- and we've heard this a few times-- but the idea that doing a solid check on the privacy and security practices of an application is somehow blocking innovation. We need to stop saying that.

PRISCILLA M. REGAN: Exactly.

BILL FITZGERALD: When we limit our view of innovation in the classroom as to what can be delivered through an app that somebody outside that classroom designs and builds, we are fundamentally misunderstanding what innovation can be. So we need to start there. Then if we're actually going to start talking about what uses of data are OK to improve a product, we should think about how a lawyer would describe that, how a student would describe that, how a teacher would describe that, and how a parent would describe that.

Because there's going to be four very different descriptions there. And our descriptions should start with what a student does to generate any data stream that's collected or generated by use of an app. And then let's just count the number of sentences, commas, words to describe how that can be used.

But yeah, if there's not a straight line between what a student does and how that data is then subsequently reused, and if there's not a clear definition of how long that data is retained, and a clear definition of how long somebody can access it, these are all things that actually have real implications for the security of data that's collected over time and how that's used. So I think if we start to get clear on some of these underlying definitions, we can come up with a better answer to what's appropriate and what's not appropriate. But until we actually start to deconstruct some of the assumptions that are buried in that statement, we're just going to go around and around and around on the theoreticals here.

PEDER MAGEE: Dan, how about from Quizlet's perspective? I understand that you're getting the consent from the parents, but how would you make a distinction on what's an educational purpose as opposed to some other commercial purpose?

DAN CROWLEY: I think that distinction, it can be hard to tease out, because you have companies whose commercial purpose is education. And so you have a company who's coming in and that is their business. Their business is helping teachers with a tool.

And so you're trying to build the best tool possible for that teacher. You're trying to build the best tool possible for that student. And so innovation in tech comes about because you have data that's come back and you're able to analyze it. You don't always need or necessarily want that data to be personal data, though. You can do a lot of innovation without it necessarily having to be personal data.

I'll give an example. At Quizlet we recently launched-- or I guess back in March we launched a new learning mode for students which was a machine-based learning algorithm that uses spaced repetition-based learning. Has a long history of success. And part of that was we were able to use actually anonymized sets of how people learned and to be able to predict when someone might be about to forget a particular piece of information based on their question history and how that matched previous ones.

And we could recommend a different question type which might be easier to them. And that was a way that we were able to improve our product without compromising personal privacy or having to dig in and understand, oh, it was this specific person answering these specific questions. And so I think there's a lot of good product improvement you can do that will help children and help teachers teach better and more effectively that doesn't necessarily compromise privacy, and I think fits well within the educational purpose of the app.

PEDER MAGEE: All right, thank you. Another big COPPA question which we teed up earlier. And this is a fuzzy area, but as we noted, the COPPA has other requirements beyond notice and consent. Those include giving parents the ability to access and delete kids' information. And I'd like to hear the panel's thoughts on the situation where when the school is giving consent, what happens to those other COPPA rights? And maybe, Linnette, you could kick this off.

LINNETTE ATTAI: Sure. I think in that regard, we have a really good model in the way FERPA has been implemented when parents want to exercise their FERPA rights to access, amend, or correct their students' education record. Oftentimes, when that data is stored with a vendor, the district will require that the vendor pass any of those requests through the school. So those requests are being made through the school so that there's a dialogue between the parent and the school.

And I think that when consent is made by the district, or through the district, there's an opportunity here to maybe look to that governance model that's happening with FERPA and say, well, if the district gave consent in lieu of the parents or on behalf of the parents, then perhaps those parent requests are best filtered through the school to the vendor, so that the school and the parent can have a dialogue about the implications of deleting a child's education record, which the school is supposed to maintain direct control over.

So it's definitely one of these areas where FERPA and COPPA do not get along. They just were not written for the same purposes and not even with the same industries in mind. But I think there is a model to say who is giving that consent on behalf of the-- if someone is giving consent on behalf of the parents, then maybe that is an opportunity for and schools to be having a dialogue about parents taking advantage of their rights under COPPA to review the data that's been collected and possibly delete it.

PEDER MAGEE: Melissa, what are your thoughts on that?

MELISSA TEBBENKAMP: I have to echo that. I think that any opportunity we have to have that conversation with our parents when they have a concern about their students data is a great opportunity for us to have that dialogue. We have a few requests each year of parents coming in and either not wanting their students to use a site, not wanting their students to use a computer at all, or wanting to just say, let's not use this set of resources.

And that gives us a great opportunity for that building administrator to build a relationship with that family, understand their point of view, where they're coming from, and come up with a middle ground. And sometimes that means that we do modify what that student's doing. But most of the time, it means that that parent has an understanding of our data governance and they become more comfortable and we build that trust.

And that's just another avenue, then, for us to build what we need, which is trust. And so having those filter-- if I am given the permission, then it should filter back through that school. Those conversations can be had. And then also, those student records can be protected in the means. If the data does get deleted, maybe we can pull down that data and make sure that we're maintaining what we need, and then find another way to collect what we need for that student's progress in whatever area that might be.

PEDER MAGEE: All right, I'm going to turn it over to my colleague to weigh in on some questions.

MICHAEL HAWES: Sure, so changing subject slightly, the Student Privacy Pledge has been a mechanism by which a number of ed tech vendors have attempted to signal their commitment to student privacy. Linnette, how effective do you think the Student Privacy Pledge has been at actually protecting the privacy of students' information and ensuring that ed tech vendors have proper data security practices?

LINNETTE ATTAI: I think I'd probably rephrase the question, if you don't mind--

MICHAEL HAWES: Sure.

LINNETTE ATTAI: --which is because I don't think the pledge was designed to ensure that vendors have-- to assess the thoroughness of a vendor's privacy and security practices. What it has done is build awareness among vendors that there are requirements. And it's set some thresholds. Maybe those are minimum thresholds.

But it's essentially set out some do's and don'ts for vendors, obligations that are fairly well aligned with some common threads of the state privacy laws and FERPA so that vendors can make an attestation that they are compliant with those principles. It is not meant to be the be all end all. It is not, and it was never intended for districts to look at a company that signed the pledge and say, OK, that piece of technology is fine.

It's meant to be a tool in the toolbox. It's perhaps meant so that-- it's perhaps an opportunity for districts to say, well listen, there are some 300-plus vendors that have signed the pledge, so maybe I will start my apps and websites that my teachers are using in the classroom, maybe I'll start with those that have signed the pledge, so at least there's some promise of a privacy and security diligence being done there. But the pledge was not meant to be a stamp of approval for any piece of technology.

And so I think it's a little bit dangerous to look at it that way. It's hard, as I think you're hearing, for schools to get the right information they need about the laws. So I think with pledges, with model contracts, and with all of these efforts, which are great, we need to be very clear with schools what they mean.

MICHAEL HAWES: On the flip side-- oh, sorry. You had a comment.

BILL FITZGERALD: I mean, one of the-- just first want to echo everything Linnette said. I mean, that's spot on, especially around the goals of what the pledge is supposed to do. And really, also what it's not supposed to do.

What I actually find really useful about the pledge is that it's a signifier. And a vendor is saying we care about these things. And because a piece of technology should never, ever get near a classroom without a full evaluation, the way I use the pledge is when I've been asked to evaluate a service that has been a pledge signatory, the first thing I look at is all of the elements in their privacy policies and their security practices that align with what the pledge requires.

And I look for the fidelity of their implementation against the intent of the pledge. And that is an additional signifier, because if there are gaps between the 10 things that the pledge asks and what a vendor is actually doing, that's a signifier that there are going to be greater gaps in other areas. So I actually used the pledge as a way to start an assessment off and say, OK, they're publicly stating they're really good at these things. So if I see anything in their terms that aren't really good at these things, I then look harder at other areas. So I find it very useful for that.

PRISCILLA M. REGAN: I was going to pretty much say the same thing, that the pledge is a useful education tool and a useful starting point, but it doesn't remove the responsibility of the school to do its research and its due diligence on that. And always with these pledges and tools of self-regulation, there needs to be some sort of audit mechanism. And to a certain extent, you've got that audit mechanism in that the school district is then forming a partnership or signing a contract and dealing with that particular vendor. But the school district has the responsibility to do the research.

MICHAEL HAWES: So I want to follow up on the topic of self-regulation more in a minute, but before that, have any of you seen any examples of how the participation in the Student Privacy Pledge at its existence in the field has actually changed business practices?

LINNETTE ATTAI: I've certainly seen the existence of the pledge and the desire of vendors to sign the pledge has built a tremendous amount of awareness. And I've certainly seen a number of companies-- I've had a number of vendors come to me and say we want to sign the pledge, but we don't think our privacy policy is quite right. Or we want to sign the pledge, but we're not sure that we're doing this thing quite right. Can you help us get there?

So I think in that sense, yes, it has been-- I think companies take it quite seriously. There are a number of companies that didn't sign the pledge right away. There were many companies that didn't rush in, because they looked at it very, very carefully. It wasn't that they didn't necessarily want to, but they want to make sure that when they made that promise, that it was true.

Otherwise, Peder's team would come and get them. And they wanted to be mindful of that. But they took it very seriously. And I think they continue to take it quite seriously. So I certainly see vendors wanting to sign the pledge, or having signed the pledge and saying, listen, we're up for renewal, can you double check our work, essentially? So I think in that sense, yes.

MICHAEL HAWES: Anyone else want to comment on that? OK, so jumping back on the topic of self-regulation, so Melissa, Priscilla, Dan, any of you, do you see more of a role for self-regulation in the ed tech space, and are there other tools in addition to the Student Privacy Pledge that you think could be helpful in this arena?

DAN CROWLEY: I'll jump in here. I think that self-regulation can be really useful. I think we've seen the COPPA Safe Harbor programs that the FTC set up for compliance there as a good model. I think those are ways that we've been able to come in and establish clear standards and programs that people can subscribe to.

Quizlet has participated in those. We will continue participate in those, not only because we think it's the right thing, but I think it helps us build a stronger program. Not just in kind of a check the box compliance way, but what are the actual right things to be doing here, what are the actual best practices, and help us continue to grow that part of our business. Because we believe that's important.

And so I think that there are a number of programs-- there's the Student Privacy Pledge. There's a number of other student data privacy seals. There's one for California student privacy, there's one for FERPA guidelines. There's others that are currently in development. And I think those are all going to be really useful.

I think we've heard panels talk about norms and the general understanding of teachers and students and parents in what data is being shared. And in the space where those norms are incredibly important to establishing best practices and not having a parent be surprised, or a district be surprised about what's happening with information. I think having a broader industry standard which these kind of codes of conduct will be incredibly useful.

Actually, I'm maybe naively, cautiously optimistic that as we have the General Data Protection Regulation in Europe, which is officially codifying codes of conduct as a compliance mechanism, that as we see the adoption of those in Europe, they will be able to be brought across the pond and play a similar role in establishing those norms and standards in the US. And so I think there is real value in having that. And I think that is something that we see it in cloud already. We see it in a lot of industries. We see it on COPPA. And so I don't think there's any reason we shouldn't see it in student privacy as well.

PRISCILLA M. REGAN: Bill and I were just laughing about this, because I said it's somewhat ironic that we're relying upon regulation in Europe to allow self-regulation in the United States. But I think that we've heard since the '80s, and since the dawn of IT and the internet, that regulation is going to stifle innovation. And I think that that is not true.

And so I think that in many of the examples that Dan just gave in terms of self-regulation, that self-regulation is under the umbrella of state laws, where they have been moving and placing certain requirements on ed tech vendors around schools. And then the way of indicating to the community that you're complying with those are through some of those seal programs and things like that.

Self-regulation, we've had this debate in every sector-- the health sector, the commercial sector, banking, et cetera, et cetera-- in terms of personal information. And I think that the bottom line is that self-regulation can be a piece of what's going on, but there needs to be standards and protocols that are established at the government level, whether that's federal or state, that help to shape and provide some uniform standards and benchmarks for the schools and for the industry. So in my opinion, and based on my research and experience, you can't rely on self-regulation to work here.

DAN CROWLEY: I'll just jump in to clarify that I don't think I'm-- when I think of self-regulation, I don't think of it as we've decided what's right, deal with it. I think that there's a reason that we're here engaging in this panel. It's because we think that there are many perspectives that are valid to this conversation.

We have one perspective, but parents have one that's incredibly important. Students have one. Teachers have one. Districts have one. Government officials have one. And so we think that a proper self-regulatory framework is going to incorporate all of those perspectives and coming to a solution that actually does meet the needs of all of those different groups. Because we're here to serve those groups as well.

MELISSA TEBBENKAMP: I'll say that self-regulation takes us to the next level. So we have legislative acts that kind of give us a framework, but we need to take that into practice. And that's where that's self-regulation and those resources that are out there that come from that really help boost us. CoSN has resources-- so we had talked about some other resources.

CoSN has the protected connected learning toolkit, which really talks about moving from compliance, which is where our regulations are, to building that environment of trust. And with that toolkit, then there's a framework behind it that really helps our districts know those pillars, everything from data governance to professional development to really auditing the practices that are happening in the classroom. And districts-- we have 13 districts, I believe that's correct.

LINNETTE ATTAI: Yes.

MELISSA TEBBENKAMP: 13 districts across the nation now that have earned the seal that says that not only do we have the governance piece, we have those policies, but we're really taking that into practice in the classroom, and we're really invested in this, and that we're taking it to the next level. And so there is a place for self-regulation. We do need that foundation. We need those best practices. But we need to go beyond that as well.

LINNETTE ATTAI: And I think from the program Melissa is describing, and she's being a little modest because Raytown Quality Schools has been the recipient of-- she is one of those 13 districts that achieved the Trusted Learning Environment Seal from CoSN. And I think one of the things that works so well about the program, and any self-regulatory program that's going to be successful, is that it came from a place of deep, deep experience in the subject matter. And the organizations that it was intending to apply to the Trusted Learning Environment Seal program was developed in collaboration by CoSN, in collaboration with leadership from 28 school districts across the country, and organizations like Superintendents Association, ASCD, ASBO.

And it is a set of publicly available frameworks and requirements for schools and districts to aspire to and to adhere to. So there's transparency. And it is really about raising the bar above compliance and getting to a place where school systems are putting tangible steps in place. I should mention Steve Smith, Cambridge Public Schools, also a recipient of the TLE Seal, sitting right in the front row.

But putting those tangible steps in place, and then being able to communicate what all that means to parents is really what it's about, to build that relationship and build that trust and have that ongoing dialogue. But I think experience in building a self-regulatory framework is incredibly important. It's what makes the Student Privacy Pledge meaningful for its stated purpose is that it came from a place, from an organization that has deep, rich experience and knowledge in privacy.

MICHAEL HAWES: Bill, you want to--

BILL FITZGERALD: Yeah, I mean, a lot of people have highlighted some of the strengths and weaknesses of self-regulation. I kind of think of self-regulation like an exercise program, like you can start it today, you can stop it tomorrow. And this is-- but as we're talking about this, I mean, bringing up GDPR, actually, is great.

Because GDPR is actually a specific set of rules that any business that wants to work in Europe is going to need to follow. I think there's going to be some really positive shifts that occur here. I mean, just because these behaviors become normalized in the business world.

For people who are actually looking for some additional resources to do the work, CoSN's toolkit is-- that's a great toolkit. Strongly recommend looking at that and using that. And also as part of our work, we've actually released all of our evaluation questions that we use when we do our app evaluations. They're available online under a Creative Commons license, so you can actually take those and modify those for noncommercial purpose.

We've actually released out a basic Information Security Primer that's also freely available online and on GitHub. So you can actually download that. You can fork it and you can modify that. The Information Security Primer was actually adopted by a university professor working with students this summer. And he actually had undergrads using the basic information security tools that we documented to do research on commonly used consumer apps.

So this is actually a tool that people can use. I mean, I actually would love to get this into high schools. I would actually love to work with high school STEM classes and train them on how to do infosec, on how to do infosec reviews. Not hard to do. These tools are out there.

And so when we're talking about self-regulation, I think a lot of it-- people actually need to make the choice to do it. I think if people are looking for a badge, I think the badges are great if it makes it happen, but I also think that we need to stop looking at external validation and make the shift to actually improving internal practice as part of what we consider self-regulation.

LINNETTE ATTAI: I agree. And actually, it's one of the things that we've found with the Trusted Learning Environment is that a lot of districts are taking advantage of the fact that the requirements are publicly available. And they're coming together in cohorts across the states. We have district cohorts in Montana, Connecticut, Ohio, Missouri's starting one under Melissa's leadership, Texas.

And the districts are coming together to support each other in meeting the criteria, not necessarily to get the seal, but to work together to improve their practices, to crowdsource their knowledge, to rely on us and our TLE Seal recipients as mentors to help them continuously improve their practices. So I think there are some self-regulatory efforts out there that are valuable. I agree with what Bill said, sometimes you want the badge.

But I know that certainly for the Student Privacy Pledge, you don't sign the pledge and then you're done. There's an annual recertification. The Trusted Learning Environment Seal, if you achieve the seal, it's good for two years and then you have to recertify. So there are these built-in mechanisms to make sure that it's not just a stamp that lives forever. But the expectation is that you're continuing to improve your practices.

MICHAEL HAWES: So we're-- want to make sure that we are able to touch on a few more topics, so I'm going to pause this one here. Also, in a few minutes we're going to be doing some audience questions as well. So if you have questions you want to submit, raise your hand and somebody will come and collect your card.

So we've talked a bunch about contracts up to this point. But I wanted to delve a little bit deeper on one topic, and that's we've started to hear that in some instances, ed tech vendors who are themselves subject to COPPA are attempting to transfer that responsibility over to the schools, and are essentially putting provisions in their contract requiring the school to comply with COPPA. Melissa, or anyone else, have you seen these provisions show up? And how would you interpret them in those contexts?

MELISSA TEBBENKAMP: I do see those provisions show up. And we do not agree to those within our district. Again, we go into really custom contracts with each vendor. And so if that's something that the vendor is trying to pass off compliance to us, then that's really-- that's a red flag for me that either they don't truly understand what they're asking for us to do, or there's something else going on that we need to dive a little bit deeper into.

LINNETTE ATTAI: I'll be very frank and succinct here. I don't think there's any statutory basis for transferring liability of COPPA to a school or district. It's not strict liability unless you have a contract with the school. It's just strict liability. And COPPA applies to the operator, not to the school.

There's just this little piece that says, you know what, the consent can happen, the school can manage the consent for you. But everything else is your obligation and your liability. So I think it's a misunderstanding, and perhaps a clever attempt from some attorneys to get through that. But I don't think it's enforceable.

MICHAEL HAWES: OK, So we've talked-- this is kind of a grab bag of topics right now as we come to the end of the session. We've talked both on the last session and this one a fair amount about resources, and the resources it takes to vet apps. Have you seen or are you seeing a manifestation of what folks have called the digital divide in this regard, that well-funded districts are able to, essentially, do a better job of protecting privacy by putting more resources into vetting these apps? Are there issues there that any of you have observed?

BILL FITZGERALD: Yes, I have observed that. Larger districts and more wealthy districts have the time and the resources and the staff to do this more thoroughly. Like full stop.

MELISSA TEBBENKAMP: I'll say we don't have a full FTE doing this in Raytown, And we manage. A lot of it is about educating our teachers. And so we spend time doing that. And they do the initial prescreening for us.

And we make it as easy as possible, a little flowchart to go through. And it kind of tells them where to go next. And at some point, it does come to us if it's collecting student information, but we've put that initial review on the teacher. We do have them attach the contract and terms of service so they understand what that means when we're signing something.

And we have them ask those critical questions. And a lot of it is about just educating and understanding that just because an app is free doesn't necessarily mean it's the best fit for the classroom, and really looking at evaluating. Sometimes I think it adds pause to signing up for that one app that you might only use for a week. But there are what I say, there are a lot of other great resources out there, so let's figure out what you really need. We're not trying to stifle innovation, we're just trying to find the best tool to do what we're trying to accomplish.

MICHAEL HAWES: Kind of on a related note, have you seen disparities in ability to negotiate for changes in terms of provisions within contracts based on the resources available in the district?

MELISSA TEBBENKAMP: Possibly at that level. I'll tell you that there are some contracts that I pass off to my legal counsel and say, I'm not sure about this provision and this provision, help me with the wording. And maybe some districts don't have that access to their legal counsel to be able to do that, because it can be costly to engage legal counsel in that. I do think that funding at that level to really help us with the compliance and that piece of it is great, because that's not something that typically funds are there for. I'm fortunate enough that we make it a priority in our district that we use those resources that way, but I don't know if all districts can do that.

BILL FITZGERALD: And there are two issues there. Like first off, I have definitely observed what you just described. But it's also-- it exacerbates another problem, which is compliance is actually the lowest bar. And it's possible for a vendor to be fully compliant and still do horrible things with data.

And if the energy is going into making sure that the compliance needs are met, there often-- especially in a smaller district, there often isn't a comparable level of due diligence about data handling and just understanding exactly what's being agreed to in those terms. So it's actually a twofold problem where often compliance gets the lion's share of the attention.

MICHAEL HAWES: All right, so I'm going to give you kind of one last grab bag question that you can interpret how you will before we jump into the numerous audience questions that we've received. So both the Federal Trade Commission and the Department of Education have issued guidance on COPPA and on FERPA. In your respective opinions, is that guidance sufficient or do we need more? And if so, what?

LINNETTE ATTAI: All right, I'll start.

[LAUGHTER]

Don't be shy, people. I think there's good guidance out there. I think there are clearly some areas where we would benefit from some additional clarity in the guidance that exists. So I'm not sure if we need more guidance so much as there are some questions about the guidance that already exists, and it would be helpful to get really more specific around that.

I think in terms of more guidance-- listen, I know schools and districts have been clamoring for some sort of explanation of how do I navigate that murky intersection of COPPA and FERPA where they don't speak to each other and they don't get along. And I'm not sure what's possible there. But I think that the more we start to think about our guidance in the framework of who has the regulatory authority for the guidance being issued as specific as possible, and then with appreciation for the fact that there is a landscape of 120-something student data privacy laws out there that we're trying to comply with.

They all define their terms differently. They all have different requirements. Same thematics, but very different specifics. And to say as much as we can find cohesion between FERPA and COPPA, such that it currently exists, I think that would be the place to maybe, perhaps, remind schools and districts of where they line up, at least to let us hook into some sort of universality among this matrix that we are all navigating through.

MICHAEL HAWES: Anyone else want to comment?

PRISCILLA M. REGAN: I think that the guidance that you've given has, on the whole, been helpful, especially the one I really like is the guidelines for the terms of service, getting specific in that way. So I think thinking of guidance as another resource for the schools and the teachers and the parents is really important. But it's the plain language. It's the same type of thing that I think parents and teachers and schools want from the vendors in terms of understanding what uses are being made of information. That plain language in terms of guidance is really important.

MICHAEL HAWES: Bill.

PRISCILLA M. REGAN: Yeah, in some ways I think the guidance that you have out is great. I would actually like to see us ask more questions. And the thing is-- and all of us here in this room, like we're the wrong people to ask the questions, because we're here. And that indicates that we've already descended to a certain depth in the privacy rabbit hole.

But I actually think we need to get questions from people who aren't here who have these concerns and figure out a way to translate those concerns into what the various laws require. Like I think that they're actually-- we do need to do more outreach to more people who have generalized concerns but don't necessarily know how to articulate them. And I don't say that lightly. That's a huge amount of work. But I think that's, I think, the next step in refining this guidance.

I also think, just to be blunt, these are two laws that are old and imprecise. I don't think either of these laws would still be in high school anymore. So yeah, that's part of what you're going against when you're coming up with guidance here, like these laws are showing their age.

MICHAEL HAWES: All right, so move on to some audience questions.

PEDER MAGEE: Well first, thanks, everyone. I think we got at least one question from everyone.

[LAUGHTER]

We won't have time to go through them all, but maybe we'll just pick a couple. One is-- and I think this actually works well with how Priscilla opened up talking about some of the privacy concerns. And the question is, are you aware of problematic uses or disclosure of student data? If so, can you give us some examples? And Priscilla, maybe you can start, and anyone else can weigh in.

PRISCILLA M. REGAN: OK, think I think it's-- I'm not going to give specific examples, but I think what tends to happen in this area, as is true in other areas as well, is that you do have a range of vendors. You've got a range of teacher habits. You've got a range of school districts.

And the kind of bad apples, if you will, the horror stories or the anecdotes that come out of where there has been misuse of information, that sort of colors everything else. So there really is an interest here in making sure that the best practices and the standards are being used uniformly across the board, because for companies that have really good policies, a company that has a bad policy is going to have-- there's an externality. There's an effect here that's going to happen on the environment as a whole.

And I think the same thing with the state laws. The ones that are good state laws. Then you have earlier the example of Louisiana was given as a state law that kind of overreached and was overcomplicated and was unclear. The same thing happens. Then people say, well, we don't need any state laws.

So I'm not sure that really answers the question, but that's one piece of it. The other is that there's an effect on this area from other areas when there are the data breaches, the Equifax. Then all of a sudden, people are very, very conscious of information and access to information and misuse of information, not just in terms of credit, but also in terms of education. So all of those can affect this area.

PEDER MAGEE: Other thoughts on specific examples or concerns, why we care about privacy in this area?

BILL FITZGERALD: I'm not going to answer the second part of the question, but I just would want to point people to the EdTech breach map. I forget the exact URL that it's at, but the person who maintains it is sitting right there. So yeah, if you want to actually look at probably several hundred, at this point, examples starting back in 2016. I mean, that documents how it happens.

LINNETTE ATTAI: But I think aside from a breach situation, a security incident, in terms of-- I think we've been hearing for a couple of years now that things must be happening with the data that aren't appropriate. And I think the question is right on target, because we still do not know what those things are that are troubling people so. We have a lot of fear out there, fear that companies are monetizing data.

If the app is free, they must be doing something with your data that's wrong. If the privacy policy isn't quite right, they must be doing something. If they are doing analytics, if they're doing product improvement, something must be going wrong. But we need to take fear out of the equation.

We need to get informed, speak from a place of knowledge. And if there are these examples of companies, schools, anyone doing horrible, horrible things with data, let's get it out in the open so that we know what it is that we're talking about and what it is that we're scared of. In terms of why privacy matters, look, we're all in the education space, we're all in the youth space.

Schools, as part of your charter, as part of the reason for schools being, it was mentioned earlier we protect the physical safety of the child. Children in our school environment are safe, warm, and secure. And we have to now extend that same ethical responsibility to their data. And that's just the world we live in.

We've always looked at, from a regulatory perspective, youth as vulnerable individuals. And we've afforded them special protections. And it's just an extension of who we are working in the education space as we're protecting children. And we have to extend those same protections to their data. It's the 21st century world that we live in.

MICHAEL HAWES: All right, so here's a question that I find really interesting. So either in schools' evaluations of privacy policies or in the various self-regulatory frameworks for establishing privacy policies, to what degree is metadata being considered in those evaluations? And in the era of big data being able to infer characteristics about individuals based on metadata, probabilistic identification of users, ad trackers, and so on, do traditional regulatory classifications of PII still make sense? Bill.

BILL FITZGERALD: Yeah, our evaluation process explicitly includes metadata. And the definition of even what metadata is will vary based on context. And yeah, I think the notion of how PII is traditionally defined is definitely out of date and ineffective. With a large enough dataset and the potential for recombination against existing datasets, it's very easy to pull an individual out of the noise.

DAN CROWLEY: I'll jump in a little here. I think the point about metadata is well-taken. I think that when we look at the data that we have, there is variance in terms of that data. And to properly-- to actually properly anonymize data is not simply the removal of a specific piece of PII. You can't just say, well, I got rid of the email address, it's anonymized.

There's a whole field of differential privacy which comes in. And you can actually understand, do I have the right level of t-closeness? And there is like actual mathematical depth that you can go into to understand if something's actually, truly anonymous or actually, truly been aggregated.

And I think it's incumbent-- I may not make many friends in the industry, but I do think it's incumbent that we make that investment to do that properly. Because if we believe that data is important to improving our products and making things better, and I do, and I think the industry does as a whole-- I don't think that's particularly shocking-- then we also have a corollary obligation to do the right thing and actually anonymize that data when we say we will. And so I think that's another step that we can take as an industry to be responsible actors in this and to build that trust with parents and with teachers and with districts.

PRISCILLA M. REGAN: And in terms of being able to do that, the size of your population is really important. And in many instances, or in some instances, it's a subgroup. So it's sort of like students with disabilities, it's very hard to anonymize or make that data non-identifiable. Or it's easy to re-identify that data.

The same thing with your gifted and talented or high achieving students. So that anytime you've got students in subgroups, it's easier to re-identify those students. But yes, definitely, as Bill started off with, the definition of PII is outdated, and metadata definitely has to be included.

DAN CROWLEY: And metadata is going to vary really widely based on the provider. I mean, the metadata that we have about a user is incredibly limited relative to what an LMS would say, or someone with disciplinary records or health records. We collect an email address and a date of birth.

LINNETTE ATTAI: There's also a vast misunderstanding of what metadata is. And we have to stop in this industry and this ecosystem between schools and districts and vendors, we have to stop throwing out terms and not defining them. Metadata is just data about data. It may be identifiable. It may not be.

And so sometimes metadata might be OK to use in a lot of circumstances. And other times it's not. So I disagree to a certain extent that the definitions of personal information are out of date. I think, actually, what we don't have is a lot of good clarity, a lot of good education on what metadata is and how it may or may not be used in compliance with the laws, as well as the existing de-identification standards that are out there in the laws. The FERPA de-identification standard is broad and wide and very hard to achieve. And it does take what Dan mentioned.

And I don't think you're alienating industry by saying that. I think this is what we all strive to do is to remove the identifiers and the indirect identifiers, and be careful about our sample size, and be careful how we combine the data, taking into account the multiple releases of data, as FERPA will tell us. So it's not a you just de-identify it and you're done. You de-identify it, and then as you're using it, you have to be careful in every use case that it remains de-identified and you're doing it right.

MICHAEL HAWES: So apparently, our timer has been lying to us and we are actually out of time. But one last thought, Bill?

BILL FITZGERALD: I agree with Linnette, these terms are not well-understood and they're not well-defined. Two examples that I find very useful in explaining what metadata is and how it can be used are both from academics. Actually one, is an academic study. One was a study by privacy researchers.

But the first study actually looked at clickstream data. People bought a range of clickstream data and were able to identify people out of that. The second is a-- that was actually originally done in Germany. And it was actually presented at Black Hat recently.

The second study came out of the University of Washington, and it showed how, for about $1,000, somebody could use the existing mobile ad tech to identify an individual based on a range of things. And this was using these advertising tools as designed, like not exploiting a bug, but using them actually as they are supposed to work. And these are really good examples, because they illustrate what metadata means and how it can be used.

PEDER MAGEE: All right, well, I want to be mindful of the time and give everybody the opportunity to have a break for lunch. We're going to conclude now until 2:15. Lunch is available in the cafeteria. I hope everyone will come back for the final panel, where we'll be looking at concrete recommendations on how to address some of the issues we've heard today.

I want to thank the audience for all your great questions. I apologize that we didn't have time to get to them. I'm sure the final panel will address everything.

[LAUGHTER]

And I want to thank our panelists. You were all terrific and we really appreciate your insight and thoughts. Thank you.

[MUSIC PLAYING]