FTC Workshop: Student Privacy and Ed Tech
December 1, 2017
Segment 2: Panel 2
Transcript

[MUSIC PLAYING]

MICHAEL HAWES: All right. If everyone could please take your seats, we'll get started with our next panel. Wonderful. So our first session was the brief overviews of the various topics we're discussing. Now we're going to move on to discussing what's in your program as the school perspective. But I think more appropriately, it could be thought of as the school and parent perspective. And we've got a great lineup of expert speakers here today.

Starting on my far, far left is Allen Miedema, who's the technology director at Northshore School District in Bothell, Washington. Next, we have Jim Siegl, who's the technology architect at Fairfax County Public Schools in Virginia. We've got Chris Pascke who's the executive director of data security for Jeffco Public Schools in Colorado. And, lastly, we have Rachael Stickland who's the co-founder and co-chair of the Parent Coalition for Student Privacy. So thank you all very much for joining us today.

So to kick things off, Rachael, you're a parent with two children in public schools. What does the use of education technology in the classroom look like from your perspective?

RACHAEL STICKLAND: First, I want to thank you for the opportunity to be here and give the parent perspective. Oftentimes parents aren't invited to these sorts of events. So it's very nice and refreshing to have the opportunity to share the parent voice. So thank you. And thank you to the FTC.

So parents are generally overwhelmed by the amount of technology that's entering the classroom. On a daily basis, your children are signed up for apps and programs. And you are never even notified, much less given the opportunity to consent.

For my own children, they are often signed up for services and apps at the beginning of the school year and actually never use those programs. Or the teacher will use them for a couple of weeks and decide that they're fairly useless, so they're not living up to the promises. And so they just sort of terminate the use in the classroom.

And so at the end of the school year, parents, I think, assume that those accounts are being closed and that that data is being deleted. But there is no follow-up by the school or anyone else to let you know the status of those accounts and whether they live on in sort of perpetuity. And then, finally, there's just no accountability for any breaches or leaks by EdTech vendors in the classroom.

For instance, my child was signed up for Edmodo when he was in third grade, signed up by a classroom volunteer, without ever notifying me or gaining my consent. And it was used for a couple of weeks during that year. And then several years later, I got an email saying that our

information had been part of the hack, the Edmodo hack. So there was no correspondence or communication from the school district. We just sort of wandered and foundered out there in sort of this no man's land.

MICHAEL HAWES: OK. So following up on that, you're a well-informed person on this issue, a well informed parent. How would you describe the average parent's understanding of the use of EdTech in schools?

RACHAEL STICKLAND: I would say that a lot of are still sort of in the zone of their own experience, recalling how education and the schools were when they were in school. And for parents my age, that was in the '70s and '80s. And so that's a lot of my peers. They think that the school records are still held in a file cabinet down in the principal's office. Or they might think that it's online, but it's in the servers that the school district maintains and that they have control over it and that there is not any third-party sharing.

So I would say generally they are aware that it's being used, but don't understand the implications. But when they do, when they are sort of illuminated, then they have very serious privacy concerns and feel like that the laws, the FERPA and CAPA laws should be protecting against a lot of things that they actually don't.

MICHAEL HAWES: Great. Moving on, Chris, in Jeffco where have you struggled with student data privacy issues?

CHRIS PASCHKE: I guess Jeffco was thrust into the student data privacy landscape as we were one of the partner school districts that were trying to roll off the InBloom initiative. So basically, in a nutshell, InBloom was going to be a large cloud service that would allow us to store student data consistently and allow us to share that data with other EdTech vendors in the form of apps or something like that, with the state, and the federal government, and with parents.

As we rolled through with that initiative, we discovered we were kind of behind the eight ball in terms of how our information security policies were written. They were written more towards data stored in our data center. Our purchasing policies were the same way. We really just had our purchasing policies focused on applications that might live on a computer or live in the data center. And we're just starting to explore how these applications were working in the cloud.

We also kind of looked at-- we knew we had a problem with data sharing. We knew that this was something that was going to grow. It was something that was going to kind of erupt, like we're seeing it now. And we knew we needed to get ahead of that. But I don't think we really grasped what data was being collected.

This has been something that evolved from the file cabinet days to tech in a data center and quickly evolved to tech that was stored in the cloud, or information that was stored in the cloud. And the information was becoming more valuable, too. It was information that was simply going from records to well-designed systems that could store a lot of data. So records would have all sorts of data potentially. And we were just kind of thinking about the old file cabinet days when data was evolving into this, what we're seeing today.

So we basically, what we were doing was as this evolved, an analogy that I thought of is our parents, in the physical space, they trust that we-- they drop their kids off at Jeffco. And they're kept warm, safe, and dry in our buildings. And that's it. If we take them on a field trip, we send home permission slips. We let parents know that we're taking them off premise.

Technology has evolved, kind of starting out slowly and now quickly, to where the data, our child's data, is no longer warm, safe, and dry in our data centers. It is now out, being worked on, and being manipulated out in the cloud. And we were behind. We didn't send home those virtual permission slips, basically, so parents were concerned about what's going on.

If you kind of fast forward to today, we still struggle with the same problems only it's more decentralized. We work with a ton of vendors in the cloud. And just managing those vendors is difficult. As we talked about before, FERPA allows parents to request student records, right? Or request, edit, and access student records.

Back in the file cabinet days, that was pretty simple. But now as these tools have evolved, student records may live on dozens of systems in the cloud, in our data centers, shared with partners. So something as simple as a record request has become very, very complicated. So that's where we've struggled, just this really quick explosion of online tech. And both our policies and statute hasn't kept up with it.

MICHAEL HAWES: So, Rachael, you were involved during this period. What can you tell us about the InBloom incident and Jeffco from the perspective of parents and the privacy community.

RACHAEL STICKLAND: I think what I learned from this experience, especially, is the powerful influence the EdTech industry has over education. You know, I've heard anecdotally and read that a lot of EdTech vendors found the normal contractor procurement process very tedious and difficult and stifled their ability to get in the classroom. And so they came up with creative and ingenious ways to circumvent that process, which is by often developing a free product, and then targeting teachers directly and sort of getting teachers buy in, and having them be ambassadors for their products in the schools.

And it's a very, untransparent, it's a very vague process. And in the case of InBloom, it was a very undemocratic process. Because it was a massively funded project by the Gates Foundation, a nonprofit organization, who was willing to develop this technology and pilot it for free to schools. And by doing so, it sort of flew under the radar of any normal processes that a normal technology project or initiative would have to go through.

So for instance, my first meeting sitting down with my district leaders, I said when did the board approve such a massive shift in the way that we are going to have our data managed and shared? And the response was we never took it to the board. This was a staff level decision, mostly because it was free. And the licensing fees would come on later down the road.

And so my biggest takeaway from the whole InBloom fiasco, frankly, was again that the influence of technology in the classroom. And then, of course, that when parents understood

what was happening, when they were told what was happening, they were fiercely protective of their children's data. And they were willing to go to great lengths and great extents to make sure it was protected.

MICHAEL HAWES: Thank you. So you talked a little bit about some of the lessons learned from that. Maybe we can explore that a little further to both you and Chris. What do you see as the overall most important lessons that Jeffco and the community learned from that the whole InBloom experience?

RACHAEL STICKLAND: I'll let you go first, Chris.

CHRIS PASCHKE: OK. Definitely like parents need to really understand what data is being collected about their students. And data encompasses a broader term than what it was back when a lot of these statutes were written. Data could be metadata. Now it could be IP addresses. It could be what types of devices do they use? Like data is a much broader term right now. And we need to understand what is being collected and we need to present that back to our families in a good, proactive way.

They need to understand how their data is being protected. That is, from my background, usually one of the easier conversations to have, because it's very concrete. You can talk about controls. You can talk about encryption and standards. But we need to understand that there are good standards in place to protect our students' data. And those standards need to apply to not only the districts, the agencies, that we're working with, and the our direct contractors, but a lot of these contractors have subcontractors. And a lot of those contractors have subcontractors. So we need to make sure that a lot of the rules that we're looking at apply to everyone who's working with that data.

We also need to really start to focus on data lifecycle. Back in the file cabinet days, data would live in a warehouse kind of in perpetuity in a lot of districts. Some districts would manage data. And others would maybe manage district data in a way where, as we're keeping a system, data would stay on that system. But as we updated to a new system, that was time to purge the student data. Like student data needs a finite life cycle and that needs to be consistent across the board.

And we also need to understand how that data's being shared. Like I said before, a lot of these relationships that K-12s enter into with either a online EdTech tool, with a college or a partner there, grants and research, or with state and federal agencies has intermediaries. A lot of times, Jeffco would be required to share data with one of our partners. But those partners use a third party provider to facilitate that sharing of data.

So we need to make sure that we're understanding how all these partnerships work and can present them back. Because many of them are very complex, so we need to present them back to our families.

MICHAEL HAWES: Rachael, anything you want to add?

RACHAEL STICKLAND: Yeah. Just briefly, I'll just reiterate what I learned, and I think what a lot of parents learned, is that our understanding of FERPA and CAPA as these federal laws that are intended to protect student privacy aren't sufficient for the 21st century classroom. They really need to be updated and clarified.

And then I think the other issue is that we need to have an honest and heart-to-heart discussion, parents, with our school district leaders about what this technology means for the classroom. What are the health risks of being exposed to screens all day? What are the implications for the pedagogy of these EdTech products that are brought into the classroom without a lot of research or evidence that they are going to do the things that they are promised to do.

So I think for a lesson for school districts and parents is to have some of those very honest conversations and make decisions upfront rather than putting parents in the position of having to opt out after the decision's been made. We should be collaborating together to decide whether or not those products and those services should be used at school at all, and to what extent.

MICHAEL HAWES: Great. Thank you.

CHRIS PASCHKE: I think I have one more that I'd like to add as we've been talking. Procurement, as well, a lot of state procurement guidelines about how districts should purchase things were designed in the days when we were purchasing like gym equipment, kickballs, or something like that for the school. So we need more guidance, better help on procurement policies, because a lot of the policies we have right now don't scale to the sheer volume of tools that we're trying to manage through.

RACHAEL STICKLAND: Thank you.

MICHAEL HAWES: Allen or Jim, have either of you had similar experiences in your districts?

ALLEN MIEDEMA: Go ahead, Jim.

JIM SIEGL: So I think there are certainly some unusual and unique things about InBloom, but I think many of us on the district side could generalize and say that there are things that are common with very large, disruptive technology projects. Like a one-to-one roll out or a shift to digital online textbooks or rolling out a district wide collaboration tool like the Microsoft tool or the Google tool. And I think a lot of those really depend on communication and setting expectations.

And I think that's true for these large disruptive projects. I think you also mentioned the flip side of that, just not the large disruptive projects, but the sheer volume of tools that are used and getting a handle around the data collection. And sometimes it's phrased as, you know, parent concerns versus district concerns. But one of the things in listening to both of you that I hear that I feel strongly about as well is both groups in order to do our jobs, we need to have a really good understanding and good quality information from the vendor on what information is being collected, how it's being used, including how that information is being augmented, how it's being

shared, how it's being protected, and how it's being deleted. And I think those are some of the things that we have in common.

ALLEN MIEDEMA: I'd say in Northshore we haven't had anything specifically like what InBloom's had, or the situation there, largely because InBloom happened, so we got to learn lessons from some of that. So thank you for that.

[LAUGHTER]

I would say that when we reflect back on places where maybe we have had problems or difficulties or stumbled, it mostly rolls back to communication and transparency. Now when we reflect back on it, we say where did this project mess up? It was not coordinating with parents and communicating with them about what was going on, not coordinating with one another within the district and within the state.

The number of times-- when you talk about the effectiveness of some of the EdTech that gets put in the classroom-- the number of times that we get a product that's gone through a curriculum adoption program only to find out that never included anybody looking at the privacy policies associated with that product is pretty remarkable. And I'm not talking about things that come out of our district office, things that come down to us from the state office. Where they've said this is approved curriculum from the state for this purpose.

And the first thing I do is I look and I see there is not-- it's not that there's a bad privacy policy, there is no privacy policy for this tool. How does adoption not include looking at those issues?

So I would say that there's nothing nefarious I would say that anybody's doing there. It's a lack of understanding this is part of adopting curriculum. Not just is it good for the classroom, but is it appropriate for the classroom also.

So I think our parents are largely-- not largely, they're very supportive of innovation and technology in our classroom. I think they just want us to do a better job adopting it. I don't get much pressure to slow down. I get more pressure to do a better job.

MICHAEL HAWES: So, Chris, you mentioned a bunch of lessons learned from the InBloom experience. Building on those lessons learned, what have you done to better address student data privacy concerns in Jeffco?

CHRIS PASCHKE: First of all we've kind of restructured the organization a little. There's myself, an individual on the EdTech side who she's responsible for data privacy. I'm responsible for data security leaning into data privacy. And then we have another individual who's in charge of data governance, as well. So we've really elevated in some roles in the organization to help enforce some of these rules that we'll talk about.

So what we've done immediately is we retooled a bunch of our processes. We retooled data management processes. We did some retooling of our purchasing processes. But like I said

before, they're still not quite there. We still struggle with that. We've also retooled security practices.

So one of the big things we did kind of start out with is we created a data governance community or data governance committee. We assigned data stewards. So we started to hold individuals accountable in the organization for data that they're collecting.

One of the big initiatives that the data governance group did was that they created data scorecards. They started to look at what is the data quality? And as you all know, we could probably spend the rest of the day just debating what a definition of a school is within each of our organizations. So that group has really had a monumental task of just starting to look at what data that we're collecting.

We're also starting to work on-- after we finish those two big initiatives-- we're starting to work on how to define data life cycles both within and outside of our organization.

So we started with governance. And then we also worked on how do we better get a handle of the EdTech tools that we're using in the classroom. So we created a standard or a process which is kind of a three-tiered process. We divide our tools into riskier tools, middle of the road tools, and less risky tools. And we work them through a vetting process where the riskier tools, we do security review, a technical kind of controls based review, which is just a paper exercise. Ideally, we would scan and we would do some more technical work. But our review is just a paper exercise. And then we apply contract language to those riskier tools.

For the middle of the road tools, we've found that it's easy for us IT security people to talk to their IT security people. It's usually a quicker conversation than lawyers talking to lawyers about contract language. So we send those vendors our 50 questions security questionnaire to help get a picture of what they're doing to protect security and privacy practices.

And then for those smaller vendors, which end up being the brunt of the vendors unfortunately, that's where the problem comes in with purchasing, again, is now it's not something big like InBloom that slips through the cracks, it's all these smaller vendors that just there's a lot of them. But with those, we have a vetted list that a central group of us looks at their privacy policies to see if they pass muster.

So through that, we've looked at about 700 different software titles, which admittedly is daunting. And that's kind of where the problems come in is how do we manage, continually, this sheer volume of tools.

MICHAEL HAWES: Great.

ALLEN MIEDEMA: Can I ask-- Chris, what's your student FTE? I worry about scalability of some of the solutions you're talking about.

CHRIS PASCHKE: Yeah. Our student FTE are, let's see, students is about 85,000 students in the district. So we have dedicated, I would say, at any one time that process that I just mentioned

very simply, we have one FTE between the information security department, the EdTech department, or the purchasing department working on this, one to 1 and 1/2 FTEs.

So the problem is is we're a big district with resources that, especially after InBloom, we've augmented our resources. Smaller school districts are dealing with the exact same vendors that we are and they don't have the resources.

ALLEN MIEDEMA: I think the majority of the districts in the country are probably less than 5,000 kids. So I worry about putting so-- and this is not to knock what you've done. If I had the resources you've got-- I'm 22,000 and I don't have those resources. But in Washington, I'm big. But I don't have those resources. And certainly Royal City and Mattawa don't have those resources. I worry that we-- if we're going to devise solutions that only set people up to be failures, that--

CHRIS PASCHKE: And even with this solution, like I said, I just said it was a paper exercise, right? Being the IT security guy, ideally we would we would look at these policies. Then we'd look at practices. And then we'd look at technical controls to meet those. So even what we devised isn't perfect by any means.

And then another interesting area that has been concerning for us is there's been a few vendors, whereas we've done our technical review, we get one set of answers. And then as our legal team and purchasing team does the contract review touching on the same topics, they get a different set of answers. So that shows that there is a lot of inconsistency in the system. And there is definitely the potential for failure.

ALLEN MIEDEMA: Which is an argument for centralizing that, right? And I would do the same thing that you've done. But when we've got things fragmented out, that's exactly-- we end up with the exact same problem. And again if I think about High Desert ESD in Eastern Oregon and resources that they've got, that's going to be a massive problem for them.

CHRIS PASCHKE: Yeah. And then this is the process. But our district also support school choice. So schools definitely have the ability to look explore on their own. And, again, like ideally let's say we're going to go strictly from an infosec perspective, it would be a much more concise set of tools, because 700 is not manageable from a risk perspective at all.

ALLEN MIEDEMA: Right.

MICHAEL HAWES: Jim, a few moments ago, Rachael seemed to suggest that FERPA and CAPA are not specific or clear enough. From your perspective, are the joint requirements of FERPA and CAPA sufficiently understood when EdTech providers collect personal information from students? Are providers and schools adhering to the requirements in practice?

JIM SIEGL: So there's a lot to unpack in that question. So to avoid the obligatory "it depends" answer, so what I was hearing-- because it's always sufficient enough for what. So kind of in the first part of the conversation it was really sufficient enough to protect student privacy. And I

think in Amelia's presentation earlier, four out of five states have passed laws to kind of extend additional protections. So I think that's one part of that conversation.

But I think really the meat of your question is is it sufficient enough for schools and EdTech providers to understand and be aware of those restrictions? And then are they following them?

And so at the school level, I think, for me the answer is in terms of understanding. It's no. I think that often there's a conversation that schools are familiar with FERPA and less with CAPA. But in honesty, my experience has been just the opposite.

I think that-- I mean talking with my teacher colleagues, they're more familiar about there being something about privacy and someone being over or under 13. I think one of the unintended consequences of the conversation around privacy in the last four years has been some people go read the privacy policy. And I think what the average non privacy geek gets out of reading a privacy is what the vendor wants you to know about their product to protect themselves under their requirements under CAPA. Which is often rarely what a school needs to know to comply with FERPA and protecting the student and often is more about the terms of service and contract law than it is about complying with CAPA. So I think that that has been one of the biggest challenges.

I think on the vendor side-- many of us in this room spend a lot of time reading EdTech privacy policies. And in general, they're pretty terrible. I think one of the things that Chris has mentioned and Allen's mentioned is the amount of time that this takes. And largely, it's because that we have to spend a lot of time answering a relatively small number of very specific questions in order to make a decision. And it requires a lot of digging through the privacy policies to figure out what those answers are.

MICHAEL HAWES: Great. So building on all of that, what practical challenges do you think stakeholders face in simultaneously complying with both CAPA and FERPA?

JIM SIEGL: I think one of the challenges is we often look at them in isolation. Someone will check and see does this comply with FERPA? Does this comply with CAPA. We rarely look at them together. And there are certainly areas where they're not specific enough and we need some clarity. I think there's certainly some definitions and differences in PII, some definitions around how each uses the term contract. I mean the Department of Ed has made pretty clear in their P-TECH guidance that contract can also mean terms of service. I have some open questions about what that means in a CAPA context.

But I really think the focus and what is most challenging for schools is around the clarity around consent. I think it's pretty clear under FERPA. I think under CAPA there are two kinds of consent in the real world. There is the relatively straightforward consent in the CAPA FAQs for when a school is contracting with a vendor and they're doing something for school purposes.

But I think that there was this door that was opened in the original CAPA language about schools acting as an intermediary that has generated language that I see in quite a number of privacy policies where the vendor, in the terms of services, designating or blessing the school to be the

vendor's agent and be accountable for CAPA and maintain the permissions and produce them if the vendor asks for them. I think the original spirit was the traditional role of the school as the parents' limited agent. And in practice, I see this as the school being the vendor's agent, at which I think is certainly a conflict.

But I also think it just doesn't work in practice. Just the logistics in terms of consent and deletion and providing parents with access to that information, I think it's kind of a backdoor form of verifiable parental consent that was never actually vetted the way that all of the other methods were.

MICHAEL HAWES: Great. So Jim or Allen or both, schools often use the school official exception to FERPA's written consent requirements when disclosing personally identifiable information from education records to EdTech providers. In your experience, or experiences, what are some of the ways in which schools maintain direct control over EdTech providers under the school official exception? And should there be more alignment, perhaps, between the school official exception and school's ability to provide consent for the purposes of CAPA?

ALLEN MIEDEMA: Let's see. I'm considering the question just a little bit here. So the way that we maintain direct control over the EdTech providers is largely we try to get involved with what kind of data gets submitted or provided to the vendor in the first place. And that's problematic because also in order to have the teacher be effective in other aspects of the classroom, we provide them a lot of information. So the teacher doesn't always need to work through us to get that information to the vendor. Or the vendor might get the information directly from the student also. So the issue that folks have talked about earlier of actually keeping track of what's all the data that the vendor has got becomes enormously complicated for us.

I think that kind of gets, for me, to some of what are our primary challenges are that we have with managing compliance with CAPA and with FERPA. And the biggest one that we struggle with is just awareness on everybody's part-- on the part of the teacher, on the part of administrators in the building, on the part of the vendors on what their responsibilities really are. I'd say that as much as we all talk about these topics, it's not on these people's radar. Even to a surprising extent, not on vendor's radar. And certainly not on teachers' and administrators'.

It's too often seen as a hurdle to getting them what they want which is access to a tool that they think is going to produce positive effect on the classroom, which for a teacher is justifiably they consider that's my primary job. And that is a hurdle that gets in their way. I'm not saying that that's the attitude that should be taken, I'm saying that's the attitude that is taken.

I'd say the other big challenge teachers have and administrators have are overly trusting in this process. So when we say that XYZ school district has started using this, so why can't we use it? Or why would this huge corporation not follow the law? So certainly, it must be OK. So I end up being a roadblock to them getting what it is that they need, which is not a great place to be in.

And the other big challenge they have is pressure. Teachers have enormous pressure on timelines, performance, mission, which is educating kids, to get these things out in the classroom. And the first thing that we do is to say, stop, stop being innovative, stop being

creative, stop using these tools, then the next thing teachers are going to do is stop telling me they're doing these things at all.

MICHAEL HAWES: Jim, how about you?

JIM SIEGL: So I tend to think of this in kind of the traditional IT controls perspective-- so physical, administrative, technical controls. And what I see is when we think of administrative controls, schools will often do this through a contract or a data sharing agreement. And I think that's probably the most common way of doing it. And from the technical side, many EdTech tools-- and I think this is kind of one of the big dividers in terms of how I think about tools-- are tools that have some kind of school level or district level, administrative council, or dashboard, or where there is a relationship where we're providing them with a data feed and we have control over the data, or we have an administrative tool that lets us view data, monitor data, delete data.

But I also want to raise the point that many of these things, especially contracts, are point in time. And most of the tools that we deal with are evolving life forms. You can come in on a Monday morning and the features have changed. And those may impact the security or the privacy. So I think it's also important to think about the kinds of controls over time, not just at the beginning.

We talked about testing, paper testing, versus-- for some tools the risk may be so important that you need to do an actual technical inspection, a packet capture, or some kind of vulnerability test. Testing is another way of providing direct control. But I it's important to think about how you do that throughout the whole life cycle of using the tool.

MICHAEL HAWES: Allen, from your perspective, what would you like to see happen that could make a positive impact in this area?

ALLEN MIEDEMA: One of the first things I'd like to see us do is for folks who have got-- time is our biggest problem I think in many cases. We don't have enough, right? But we've got some folks in the conversation that do have more time to vet these tools. And here I'm thinking about statewide ed offices, EdTech publications, these places. Stop touting tools as being awesome when you haven't even looked at the privacy policies, because teachers read these things and get excited about it, and go to conference, and say, boy I want six pounds of that. That looks fantastic. Let's get that.

And then, they come back. And all I do is get to be the bad guy and tell him you can't use it because these guys actually don't have anything that approaches a legal agreement in place. So the state offices, the EdTech publications, you have time to vet these tools. Vet these tools.

The other thing I'd like to see more of is professional development for teachers, administrators, and support staff around legislation and best practices in this area. I get to go to a lot of EdTech conferences and education conferences. And I can't remember the last EdTech conference I was at where we didn't talk about privacy. And I can't remember the last ed conference I went to where we did talk about it where the room wasn't just full of EdTech people. So I think that the educators don't get enough information around this.

And the next thing I would say is take control of vetting these out of technology departments. I mean I don't know-- maybe every district in the country is different than Northshore, but I suspect it probably isn't. When information comes in and out of technology, teachers see that too often as synonymous with stuff I don't need to understand, because I don't understand how networks work. And I don't understand how routers work or what a switch is. So when they start talking about CAPA and FERPA and privacy, that's just more stuff out of tech I don't need to understand.

Put it in instruction where it belongs. That's the group who should be vetting this information. Information isn't in and of itself a technology item. So why are tech directors the ones who always are vetting these things? I've never understood that. Small rant.

I would say we need to recognize we put solutions in place, the vast majority of districts are small. And they don't have resources. And if we put legislation and processes and procedures in place, but they have no capacity to be successful on, then we are going to guarantee their failure. And one of two things I think in a broad sense is going to happen. They are either going to stop using technology or they are going to stop telling us that they're using technology. And both of those are bad

I think we need to put solutions in place that have a positive outcome, that encourage people to use technology in the classroom in positive ways. I think that Steve Smith-- I'm going to steal his thunder a little bit here-- the idea of a model contract that Steve's going to talk about, I hope, is going to be useful. I think vendors putting clear information in their contract. Jim talking about having to cipher through these contracts to find out the answer to really about six or seven questions is an incredible task.

And I'd say from a resource standpoint-- and this is kind of across education in general-- if we're going to have people vet these contracts, make it an FTE to review this stuff. Education relies so much on people providing volunteer hours, at the end of the day to read contracts and go through these processes at their kitchen table, it's not sustainable. I mean if we're going to be serious about this, then let's get serious about this.

CHRIS PASCHKE: Can I ask a follow-up question?

MICHAEL HAWES: Sure.

CHRIS PASCHKE: Have you been able to kind of charge up that hill with holding the EdTech teams more accountable for the vetting themselves? Because that's an area that we struggle on too is like--

ALLEN MIEDEMA: But, no, I fail miserably on that.

CHRIS PASCHKE: OK.

ALLEN MIEDEMA: No. I try to push back on-- what normally happens is I'll have a contract that will come in. And here I need to be clear in case anybody back in Bothell is watching. I'm speaking for myself and not for Northshore School District. I want to be employed next week.

[LAUGHTER]

I would say that I push back on these contracts at sometimes. And sometimes that's effective. And I'll say we just can't do business with these folks. I've tried to negotiate and we're not getting anywhere with them. And sometimes that's successful. And other times I end up with somebody in my office trying to explain to me why we need to go forward with this product anyways. And though they don't show me the org chart, I got a sense of where I sit and where they sit.

CHRIS PASCHKE: You know we have similar struggles. A lot of times, when we're doing like the risk work, we'll look at something that maybe a vendor might not and encrypt-- which is horrible to say-- but they might not encrypt user credentials. Those conversations are usually pretty easy, because it's pretty easy to present that back to the organization to say, yeah, this is just flagrant foul. Like this is not something that we want to put in our environment. But we struggle, as well, with some of those more gray areas where how do you really manage the risk of using these tools versus the educational benefit.

ALLEN MIEDEMA: Right. I mean so much of a contract comes down to a trust relationship, right? Where it's an issue of I don't have a relationship with the vendor that this teacher has or this administrator has. And they think Bob or Cindy are good guys and they won't do bad things. And so they trust them. And all I get to look at is the black and white of this and say this isn't descriptive enough of what they're actually doing. I'd like them to flesh this out. And it can even be that the vendors say, well, we will. That's a six month cycle. In the meantime, I'd got this teacher who would really like to use this tool on Tuesday.

CHRIS PASCHKE: Exactly. And like you said, so it's trust at one point of time, because we can't look at everything omnisciently forever. So that's where we struggle, too, is let's say if there is one vendor that we're working with, what if they get bought or sold by one of their parent organizations? Or if they change their practices?

ALLEN MIEDEMA: Has that ever happened that some gigantic corporation comes in and buys this smaller company and suddenly everything's different?

CHRIS PASCHKE: Yeah.

ALLEN MIEDEMA: I've never had that experience.

CHRIS PASCHKE: No, never at all.

JIM SIEGL: If I can, I just want to--

MICHAEL HAWES: Oh, please, please.

JIM SIEGL: --chime in with a slightly different take. So I often kind of split the difference and take the middle of the road. So I would be concerned about shifting all of the vetting onto the instructional side. I think that IT has an important role. I think IT generally very good at looking at risk. I think it's really needs to be a shared governance. I think that's been what's worked well in my experience.

I think that having the instructional folks look at the educational value and also holds the vendor and the purchase up to what the expected outcome is. And I think IT is good at looking at the risks. I don't necessarily want all of my instructional people to become legal experts.

The other thing is-- you talked about tech conferences and instructional conferences-- in any of those, in any of the conversations, of the last four years, I have rarely seen or heard mentioned anyone that lives in the procurement world in a school. They're rarely involved in the conversation. But they're typically the gatekeepers to the contract. And often we rely on the contract to be one of the forms of direct control.

ALLEN MIEDEMA: They kind of end up being our salvation, right? Because they hold the purse strings. And that's where we get to stop it and say it doesn't go forward, you get a good relationship with your procurement people and say they can be a real ally. Yeah.

JIM SIEGL: Absolutely. And I've seen that work. So I think in terms of not necessarily wanting a world where it gets pushed off all to the instructional people, but I think this is a triangle with different roles to play. And I think just as I like I don't want my instructional people have to become IT risk experts, a lot of times for the last four years, IT has taken a lot of the work of becoming contract laws experts. So I think it's kind of balancing that.

And you talked about vetting and time and what you'd like to see. I mean I think important the limitations of time that all of us have, whether we're small, medium, or large. But one of the things that we spend all of our time on is trying to sift this information out. So what would be most useful to me is rather than make the review and vetting of a privacy policy a scavenger hunt-- with many of the other things that we have in our world, whether it's the school buses or the hazardous chemicals or the food that we have in the cafeteria, they have material data sheets.

They have nutrition labels for products that we look at accessibility. We have voluntary product accessibility templates. There's a very small number of questions that you need to answer to be a school official and to answer the questions that we're supposed to ask under M5 of the CAPA facts. That's really it's 11 things that we need to know. It shouldn't be that hard to provide those things to schools that would significantly speed up our ability to do reasonable vetting.

ALLEN MIEDEMA: I absolutely agree with everything. The idea that a vendor can't give me a list of what are all the data elements you use? I mean, if you can't answer that question, we shouldn't be using you as a product. You don't know what data elements you're using? Then we shouldn't use you.

Who are the other vendors you're working with? If you don't know the answer to that question, we shouldn't be working with you. That seems like such an easy thing to provide. And I would

be-- we have a small number of vendors who do basically give you that. That is so easy. I mean it's like it makes my day, that's how bad my life is. I see something like that and then I get excited about it.

RACHAEL STICKLAND: But if I could just interject from the parent's perspective, our schools have shrinking budgets. There's so few dollars that are actually going in the classroom. And so to the extent that we can shift some of this financial burden back to the vendor community where it belongs, as opposed to in the IT departments to have you vet these contracts and try to understand and decode what are in those privacy policies, parents want that. They want money freed up for the classroom. We don't want it tied up in with lawyers and your procurement processes and in the bureaucratic processes. We want those dollars freed up.

MICHAEL HAWES: So that's actually a great segue to my next question. But before I ask it, in a couple of minutes, we're going to be taking some questions from the audience. So if you have a question you'd like to submit, please raise your hand and somebody will come around and collect that from you.

So I was going to address this one just to Chris, but I'm actually-- given the interest from all of you on this-- I'm going actually just make it an open question and any of you can comment from your perspectives what can states or the federal government do to better assist schools and districts with navigating the various challenges you've been talking about

ALLEN MIEDEMA: I felt like I was just talking about that. So I would say I would actually like to see a model template format in which to present the information that we need so that we can make these assessments and not have it all buried within legalese. To me, I'm so naive as that doesn't seem like a complicated thing to do.

CHRIS PASCHKE: I guess for me, like the first thing, is we need a little more concrete regulations like something for us to actually measure against. Colorado privacy law is very verbose but it is built on three terms-- school service provider, contract provider, and on-demand provider. And then Jeffco and some of our peer school districts, we've spent weeks and even months debating what are the definitions of those three simple terms that the rest of the law is based off. There's lots of room for kind of ambiguity, lots of room for some loopholes. And it doesn't help to build trust with our parents like it should. So we need more help, maybe more of a control-based approach to dealing with this.

And then as I kind of quickly shift over from privacy hat to security hat, as I go to different information security conferences, an upswell in the information security community is the control-based approach that I was just talking about, some sort of measurements isn't working for them either. Right?

PCI is out there. It's a control-based way to measure how we're protecting credit card information. And it seems like every week, there's a new very large organization that's getting hacked that are perfectly PCI compliant.

So not only do we need regulation, some sort of central measurement, but we need good guidance to kind of help educators or us IT professionals help decipher some very concrete terms into risk management practices. So we're not just checking some boxes off of a law, but we're really actually starting to have some good discussions around risk and then help us to be transparent with the community.

And then I think a lot of that would have to-- I agree with Rachael-- fall in the vendor's hands. It would make our jobs a lot easier if vendors simply put on their websites what data they're collecting, who are their partners, how long do they store the data, what do they use the data for. It would help not put us school districts in the middle of these technical versus contractual conversations and consistency issues. It would just be in the vendor's hands. So if it was more of a federal approach to that and more really focused on enabling parents make good choices or help enabling parents to help school districts make good choices around how that data is being used and shared and processed by these large organizations or small organizations.

JIM SIEGL: I certainly think that having clarity on the volume of state level laws that have been passed over the last couple years. Simply just having one place on a State Department of Education website to go where there was a list of all of the laws that applied to school districts regarding internet safety, student data privacy security, data breaches, data retention. That would be incredibly helpful.

Model policies and guidance, that's something that was in the legislation about two years ago in Virginia to come up with.

Training, I think, is incredibly important and something that is really given short shrift in schools. And some of it just comes down to this stuff is confusing and sometimes you need an answer to a question at the state level. At the federal level, I think districts have benefited greatly. And Michael did not pay me to say this that from the resources and the guidance of being able to pick up the phone and call P-TECH and get an answer to a question, the complexity exists just the same at the state level. And we have just as many questions.

RACHAEL STICKLAND: And I'll just say briefly, you know, we hear from all the time who want to ask for their-- request access to their education records. And their schools come back with varied responses. Like this is a FOIA request. This is in Colorado, it's called a CORA request-- and it's subject to fines or fees in order to fulfill those requests.

So having a good understanding, giving parents clarity in terms of FERPA of what is an education record. Because it's so vaguely defined, everybody kind of comes up with their own definition. And also a school official, it's not always clear who is a school official. And districts aren't always very transparent with their definition of that and what constitutes a legitimate educational interest.

And similarly with CAPA, some of its vague language, we have parents reaching out to us saying, well, you know, this product is used in my schools, isn't this a commercial purpose what they're doing with the data? And it's very difficult for us to help them interpret what they're doing, what this vendor might be doing, and if that constitutes a commercial purpose under

CAPA. And because our agencies are so inundated and under resourced as well, parents have a difficult time getting quick responses from P-TECH and other organizations.

So we just need clarity. We need these laws to be modernized. This industry is moving so fast and we're just not keeping pace with that.

MICHAEL HAWES: Good. Turn to my FTC colleagues. Do we have any audience questions? Wait a moment while the cards approach the table.

[LAUGHTER]

Thank you. All right. See what we've got here. OK. We've got a question for Chris here. You perform a paper check on the vendors. How does Jeffco protect itself and students in the event a security incident happens?

CHRIS PASCHKE: We include that in our paper check where we-- both on the contract side and on the technical review side-- where we on the technical side, we'll ask them what-- we'll basically tell them they have to inform us, Jeffco in the event of a breach. And they have to work with us in incident response. And then on the contract side of things, we reinforce that with contract language that says the same thing. It goes into a little more in depth.

So basically, we require vendors to work with us through the incident response process. We haven't tested that in practice yet, but that's what we have in our technical review and in our contract.

MICHAEL HAWES: Great. So here's a contract question. What if a contract or privacy policy promises that data won't be sold, but then says it can be sold in an asset sale. What's the difference and how do you treat that?

CHRIS PASCHKE: We cover that in our contracts as well where that would be a case by case basis. Our generic language would prohibit that or allow us to control that. And, yeah, so that's basically what we do in that situation. But that's something that we've addressed. We know that that is definitely an issue where if a vendor gets bought by someone or if a vendor goes out of business, what happens to our data?

MICHAEL HAWES: So I'll address this to the whole panel. You guys can chime in as you want. If parents have control, how does the vendor know what the school wants? Particularly where FERPA and state law require vendors to comply with school instructions.

RACHAEL STICKLAND: Can you repeat that, please?

CHRIS PASCHKE: I am grooming that sentence.

MICHAEL HAWES: If parents have control, under CAPA-- I think that's implied there-- how does the vendor know what the school wants-- when using a tech in the classroom-- particularly where FERPA and state law require vendors to comply with school instructions.

RACHAEL STICKLAND: I'm going to pass that on down to you guys.

MICHAEL HAWES: I think my understanding-- if I can interpret the question here-- I think it's at that intersection of CAPA and FERPA. If ultimately the school is acting as the parents' agent, I think the question is where does the parents' rights stop and the schools' rights begin would be my interpretation of this questions.

JIM SIEGL: So I think this is definitely one of the fuzzier areas. And I think it gets to some of the questions that you asked about the intersection of CAPA and school officials. And I think you've got those very two distinct cases where, in CAPA, it's very similar to the school official exception, where it's only being used for school purposes. And it's done with a contract and clearly not for any other purposes. And then you have the other case.

I think kind of the example that comes to mind that the FTC has written about was the testing piece about how CAPA applies to some of the Common Core tests, which are definitely things that are part of the school record. And I think that's one that probably needs more clarification, because I think kind of the guidance leaned towards more saying that it didn't apply because it was a nonprofit rather than that it was addressing the potential conflict between the two.

But I think the important thing is that it would be very difficult for schools to conduct business if there was this fight between who has control on data. We can't just have records being deleted from the student information system.

MICHAEL HAWES: So I've got another question here. Do you struggle to reconcile a desire to use free or low cost education technology tools with prohibition on advertising or commercializing the EdTech service?

ALLEN MIEDEMA: Oh, absolutely. I mean of course it's a massive issue, right? Because none of these tools are free. I mean we all say that all the time is that if you're not paying an invoice, then you're paying in some other manner for these services. They're not free. These people who produce these products are buying groceries every night. I mean there's some kind of monetization of this going on.

So we try to discourage our teachers from going down that route. But, ultimately, we know that for every paid service that's happening in the classroom, there's probably 10 free services that they're using out there.

And some of it, I get the motivations. It's free. Right? And an individual teacher doesn't have a budget. So they think, well, I'm going to look at this, or I'm going to explore it, or I'm going to examine it. There's not a good idea or a sense of once you provided that service data about your kids and you walk away, the data stays there. And there's just not a great awareness of that. So, yes, we struggle with that all the time.

RACHAEL STICKLAND: Yeah. If I could just chime in, too. I think schools have a responsibility to tell parents that and educate them, because many parents are from my generation again. And we love technology, but we're not very aware of-- we are OK with

convenience in return for giving up some of our privacy. And I think parents for the most part, think that these apps, these educational apps, they have a different standard applied to them than commercial or consumer apps.

So there's this kind of like underlying assumption that, gosh, if it's being used at school, there's no way that this free app is using my student's data in a commercial sense. So I think it's important for parents to understand and teachers and schools to communicate to parents that when we're using free apps, they really aren't free. And that, you know, it's fundamentally parents, I think, if they understood that it would be a big problem because these are compulsory environments. We're using public school dollars, or public dollars, to fund our schools.

And here we have students generating all this data. They're basically product testing for these vendors. And it's a really inappropriate environment for that to be happening, especially when there's no effort for the vendors or schools, in particular, telling parents this is what's happening. There's a big knowledge gap there.

JIM SIEGL: Just a quick follow-up because, well, the two of you here for Colorado, you have that term on demand service provider.

RACHAEL STICKLAND: Right.

JIM SIEGL: Has that helped this, hurt this? Has it added any clarity to this free situation?

RACHAEL STICKLAND: Well, the interesting thing about the law is it doesn't-- school districts had until December 1st of now, today, right? Yeah, to comply. And really, Chris mentioned that school districts are applying their own interpretations to these terms, even though they're fairly clear in the law.

And so today, we'll see on our school district's website, hopefully, how well they're complying with the law and if this is going to have any meaningful change in the classroom. Up until now, it has absolutely not. Yeah.

ALLEN MIEDEMA: You know, I'll bring up another sort of a variation on free. The product itself isn't free, but it comes as a grant. Or in our CTE programs, it will come with a package that somebody in the industry is providing because they're trying to do good things in the classroom for kids. So I was actually reviewing one of these contracts on the plane on the flight out here. It's a tool that's not focused on K-12, so CAPA doesn't apply. The super legislation in Washington doesn't apply.

It's really it's focus of industry. That's awesome. These kids are going to be using industry tools in this CTE class to do good things.

But this is a whole group of software that I normally wouldn't have reviewed because there's no procurement with it. And doesn't really apply, because these-- I mean to the legislation tools that I have, because it's really it's an industry based tool. And I looked through the privacy statement on this thing. And it's like two paragraphs long. But this is what sold in the real world. And you

want kids to be educated in the real world. In the real world, these protections don't exist for consumers.

MICHAEL HAWES: So we are just about out of time. But before we wrap up this panel, I want to give each of you-- kind of starting with Rachael and going down the line-- 20 or 30 seconds to give your kind of final thoughts, what you'd like folks to take away from this discussion or anything else that you didn't get a chance to talk about.

RACHAEL STICKLAND: Well, first, I just want to start, again, by thanking you for the opportunity to be here. Including parents in the conversation I think is one of the most important things that schools can do. And involving them in the decision making process. We are a stakeholder. We are perhaps the ultimate stakeholder. And we should be having conversations about the efficacy and the research behind a lot of these EdTech products before they are brought into schools. So that the consent piece happens on the front end rather than sort of forced consent on the back end, where you're having to pull your kid out of programs or school activities that are already so far down the road, so your child is missing out.

So sort of my takeaway, or I hope everyone takes away, that parents are your allies. We want to trust our schools. And please engage us in conversation.

CHRIS PASCHKE: And I'd like to echo that thanks for the invite. And I think what we need to do to help be good allies with the parents is just some more concrete guidance to stand on. So we can have better conversations instead of debating what a term means in the law. And then, really, we all need to help kind of focus on managing through that choice, all the choice that we're getting right now.

Choice is a good thing, but it's also something that we have to manage through as adults. And we have to teach our how to manage through in the classroom. And we also need to work on just making sure that we're being as transparent as possible with our families.

JIM SIEGL: I think getting more clarification on guidance is important, but I don't want to be lost in that that really we're talking there about compliance. And that's important. But it's pretty much the bottom. And in a school when we look at adopting technology tools, we're looking at compliance. But we're also looking at privacy and security and safety. And often those things kind of get lost on the are we meeting and complying with this particular aspect and checking off on the privacy policy. And I think thinking about it in the bigger picture I think is important.

ALLEN MIEDEMA: I would say that so we find ourselves in a time when we have unprecedented access to resources and opportunities to differentiate instructions for kids, to pull the focus of instruction away from the teacher and more towards kids in the classroom. And I'd say that's a great thing that we should be doing that. We should do that. And I'd say that technology plays a critical role in us being able to do that. However, we have responsibilities when we bring those kinds of tools into the classroom. And I think in large part in the education community, we've abdicated our responsibilities in those areas to too great of an extent.

And I just think we can do better. But when we do better, we've got to make sure that we don't crush innovation and opportunity for teachers and kids in the classroom. I see and hear too much of the direction that people are going into, sometimes it's to legislate to the point that, like I said earlier, teachers are either going to stop using tools or they'll just stop telling us they're using tools if we make it too complicated.

MICHAEL HAWES: Great. Well, please join me in thanking our distinguished panelists here for a fascinating discussion.

[APPLAUSE]

And we're going to be taking a short break. We're going to reconvene again at 11:40. We'll have our next panel exploring student privacy challenges, followed by lunch. Again, please remember that food and drink may not be brought back into the auditorium. Thank you.

[MUSIC PLAYING]