Project Completed by:

EDUCAUSE
Privacy 2020: Where Have We Been and What’s Next?
Thursday, January 28, 2020
1:00PM – 2:30PM Eastern
>> Welcome to today's Educause webinar. Privacy 2020 where have we been and what's next? This is Brian Kelly at Educause, and I’ll be your moderator for today's event. You are probably familiar with our interface, but we hope you'll join us in making this session interactive. Use the chat window on the left-hand side of the screen to ask questions and make comments. Use the hashtag and if you have issues click on the link at the lower left-hand side of the screen and you can submit a private message by clicking the right-hand chat window and you can select start with and host. The session recording and slides will be archived later today on the event site.

Now let's turn to today's presentation. Data privacy day it's important to exam how technology has evolved in the past decade and get ahead of privacy challenges to come. Today we'll reflect on privacy lessons learned and best practices inside and outside of education and discuss how it could impact higher ed and suggest ways that institutions can prepare for those challenges. We are delighted to be joined by the director of youth and privacy at the future of privacy forum. Amelia's policy makers, academic and institutions on child and student privacy laws and best practices. She oversees the education privacy center website and the review of applicants to the student privacy pledge. She can move stakeholders to ensure privacy use and student data and technology in schools. She is a regular speaker in education privacy conferences in the U.S. and abroad and has testified before congress and spoke in federal trade workshops and is a part of experts reviewing revised recommendations on protection of children online. She is a member of Virginia state bar and the international association of privacy professionals. Thank you for joining us today and with that, let's begin.

>> Thank you so much and thank you all for sending your data privacy day with me. That was a long intimidating bio. But really I focus on how I can best help all of you when it comes to student privacy issues, most recently been doing a whole lot with child privacy issues and my organization is the future of privacy forum is a nonprofit where we work on a variety of consumer privacy issues from education, to child privacy as I mentioned but also ai and connected cars and drones pretty much, anything that you can think of. So I’m going to a big question of the day. Is privacy dead? I hear this question a lot when I’m talking to people. So I think everyone in America feels like we do have a privacy problem. There's a new headline often every day, talking about new potential violations of privacy. And so the question really becomes, is this worth talking about? Should I take up the rest of your hour? Is this something worth spending institutional resources on and I want to do a really quick experience to really open up the question. So, close your eyes. Don't fall asleep. The year is 2020 nine, the hottest new technology is the brain machine interface. The brain machine interface also known as the BMI captures all your thoughts, all your actions and by default hosts them on twitter. You changed the default. Why or why? What are you thinking about? What have you seen on social media?
What's happening at home? What are the things that you wouldn't necessarily be comfortable with sharing? It's really important when we're talking about privacy to realize that we still do have a significant amount of privacy in our thoughts, we have a significant amount of privacy when it comes to what we do in our homes, with our friends, with others but exactly what the scope of that should be and how that might be in danger based on new technology is something we see more and more of but privacy is definitely not dead and in fact, there are many technologies that while contributing to privacy tension has certainly not killed it off. So, it's worth noting that tensions like surveillance in law enforcement, online and cross device trucking, marked home, connected cars, ai, all of these are pushing in on privacy norms and expectations at once. No one is operating independently in the information world. But what even is privacy? It's such a concept and I always like going back to professor dan's book understanding privacy and if you are not familiar with it I highly recommend reading through it. Professor goes through the many definitions of privacy but also scholars and legal frameworks and boils this down into this taxonomy. For anyone like me feels like they don't entirely understand this chart, I give you this other chart that I found. I won't go through all of this now but this is a great chart from the national university of Ireland and he defines the info of taxonomy in I think an easier way. We have information collection. So when information is being passively or actively taken from us without ourselves, without our activities we have information processing which can raise privacy concerns through information about us being collected from various sources, linking back information to particular individuals, where you go, what you do, insecurity of that data, potential secondary use of that data, data being shared with someone else, not letting people know about how their information is being processed, the why category of information dissemination, revelation of information about a person that impacts for example the way others judge who you are, revealing private information such as nudity, bodily functions. Having information possibly used against you such as through blackmail. Appropriating your information to serve the interests of another and then invasion of information. So more than just passive taking of information about you but invasive acts that may disturb tranquility or solitude: so some sort of encouragement into your decisions regarding private affairs. So we have all of these many, many definitions of privacy but we just have one word, privacy, that's being used as a proxy for all of this in newspaper headlines and in the complaints that I’m sure many of you get. But it's really important and I think if you take away anything from today, it's that more and more these conversations are not really about privacy. So this is a quote from a current fellow, the program director at privacy international and she says that privacy was once construed about hiding and secrecy but now it is understood to be something more precedent about Hower Dynamics between the individual, the state and the market and that protection speaks to mitigate the entire power and balances between people and those that collect and profit off their data. A lot of times when much of what happens in the world is being played out on browsers, on phones, with text platforms, with data in different ways, mediating the way we react, how we have elections, how we influence each other, how we teach, how we judge, how we score, how we loan, how we learn about each other, how we date, are all problems of society which are not unique to technology, many of which we have still not resolved in the offline world. We are led to legally discriminate in certain ways. Areas where we recruit and hire differently and when
these issues play out online, they are sometimes exacerbated or exposed. Analyzing which employees are going to be the best employees using historic information and using that data to decide on who to hire or promote and when they did this some of the factors were do you play lacrosse and things like that and it was clearly biased. But of course, what actually was being exposed was this is what hiring managers and others were doing, are doing, without technology. People hire people like that and are leading to fewer opportunities to minorities and the technology is exposed. Another great example was when Amazon rolled out the fastest delivery. It turns out using that data meant that there were areas that were unlikely to have a large population of minorities and Amazon said we'll run it differently but what a challenging problem. We say to retailers, don't open up next door, the place you will sell the most products the most quickly mandate throughout society? I think you should make sure people from all communities are being served but for better or worse that's not what we've chosen to require from offline companies. Data is often being used as the touch point for one to say something shouldn't happen because of privacy but what is meant is that it is not fair for you to make that decision about me or I don't trust this powerful institution. The schools, the leadership, the universities, the government, the big companies, I don't trust that this entity that is removed and sitting in an ivory tower or even an academic researchers will really do good for my community or really know me. So a lot of this is a matter of trust. It's about power and equity and fairness and discrimination and today talking about these are so often the places where the effects of these power dynamics are exacerbated. In education you can see this clearly more than anywhere else. The groups that are most concerns are made up of people worried about how they or their child will be looked at fairly. Privacy is one way to say wait, you shouldn't have that data because you are going to use it the wrong way and some people who bring up privacy concerns may be very happy about our use in a way that clearly benefits them or in a way that supports their beliefs but also calls for privacy when data results in outcomes that don't support their beliefs. So if you think that by doing privacy compliance rights and minding your P's and Q's that your institution will be fine, one lesson that I want all of you to take away from today is that you will not -- privacy compliance is just the stake to show you know the basics of how to manage the data but that compliance will not stop you of being accused of violating privacy norms. However, not having compliance down pat means that whatever you are doing at the institution, whether implementing a student success program, adopting new technology or finding new ways through technology to recruit a diverse student body, those things will be undermined, you didn't have the right policy or this or that compliance issue but it's equally vital to make the case for whatever you are doing after making sure you ensure privacy practices. So many times in the work I do I’ve seen the most well-meaning people shocked when someone says to them you are a bad privacy actor because they think that they’ve got your best interest in mind and therefore, people should give them the benefit of the doubt and well, privacy isn't just about the definitions of privacy. It's about trust and getting stakeholder buy-in. But let's go ahead and share out just a little. What's happened in the past ten years? I promised you some 2020 lenses to look back here. The iPad was first introduced to the world in January of 2010, a flood of android tablets followed after. The first smart watch popped into existence in 2012. You had an entire line of smart watches and in 2014 you had VR with risk raising 2.5 million. You have so many different
technologies as well as the development of the million and one apps that add to this personal computer, we all keep in our pocket. You also had some things that didn't go so well so we have Google's lap. In 2013 it feels like this was way more than seven years ago. The next level didn't work. It felt creepy. It was a bit much. A really interesting takeaway that someone provided and wanted to sort of decade end articles that I thought was useful was this is the age that computers became the boss of you. Where we really became a data driven society focused on data everything. Focused on having our devices know us and provide us with data about ourselves and others in order to data everything. And this is just the past ten years. There's been a massive change in society and I think it all feels like it happened really gradually and that we've had phones in our pockets forever and that, you know, google translate must have come out at least fifteen years ago but no. All of this is pretty recent. All of this is pretty new and it's important to really remember how much has changed. I also before I go into talking about some of the privacy issues, we've seen want to know that that can contribute to privacy which is not something often discussed. So you can now search google. You can google and have been able to for a good twenty years now and how do you know if you are pregnant and you are able to potentially find communities, my boss loves bringing up the advantages of the e-books and e-book apps and how people can read fifty shades of gray or whatever else they want on their device and not necessarily feel judged. Or they can learn about something where they might have saved judgment from communities, whether that is religion, politics, whatever it is. We've seen tech contribute to people being able to have more intellectual privacy. More ability to ask and explore sensitive topic areas with this tech. I don't want to take away from this to be that this is all bad. But we do have these violations that are appearing more and more on the front page. So, for anyone who saw this, this is from 2017, that's like tweeted out to the fifty-three people who have watched every day for the past eighteen days. And I think everyone did see quite a bit of engagement. I remember seeing it and laughing. But for a lot of people either in their first reaction or their second reaction was this header, Netflix creepy tweet, companies aren't just providing us with a product. People are paying for that product and collecting data from us and while our Christmas prince example feels innocuous, the fifty-three people who feel judged, this is a wakeup call for some people to remember that there is this data out there that we don't have access to that's being used for judgment by individuals and we don't know how that works. I don't know. I don't know about any of you but after this tweet I ended up going to Netflix's website and tried to find my viewing history because I was curious about the number of times I watched it on Netflix and it wasn't available so this data wasn't available. It was only available to the company and it was obviously not something that they were reluctant to share with the world and so it makes you feel a little uncomfortable. You know, how did we get there? How this being used can make massive important decisions. We love and use text on a day-to-day basis, relying on data all day with search, social media, phones, but we are edgy about what can go wrong. Examples here, what happens when life insurance companies track your fitness data? What happens when an algorithm cuts your healthcare? These are all things that unfortunately are happening in some cases. Finding friends with computers, predictive policing, the future of law enforcement. Reading resumes and in education you have essays written about ranking prospects with student tracking. You have the case where Saint Mary’s where not really using tech in a
way but using data from a rather unscientific survey to try and weed out students who are likely to fail out. These are massive decisions. These are decisions that affect our lives, our futures, our children if we choose to have them. Again, this isn't about privacy. It's about power and who has it and transparency and how much we have as we're feeding data or as others are feeding data into this system knowing we are unknowingly. And most important not only is tech being used to make big decisions there's often no respect for the context of how and why that information was provided in the first place. So really great article that was posted recently in New York times, with fabulous reporter Kashmir Hill is about a company that took facial -- took pictures from everywhere on the internet and this software allegedly allows you to take a picture of a person, upload it and get to see photos of that person along with links to wherever those photos appeared. The system which is built with a database of more than three billion images of this company, claims to have scraped from Facebook, and millions of other websites and far beyond anything ever constructed by a government, by big tech companies. It's currently only available to local cops, FBI, etcetera. But it opens up so many questions and I don't know about you but it makes me really nervous about those pictures on Facebook, those pictures on twitter, those casual pictures where I posted my cats and requests for pictures of cats to make people smile and what information is in those pictures and who is scraping that data in order to use it for something like this, essentially a tool that could end your ability to walk down the street anonymously. And the thing is, a lot of times when we have such lack of respect for context, it's because we weren't necessarily adequately informed in the first place. So another great article that came out recently in privacy world talked about location data. This is a recent screenshot from my phone where I had downloaded Angie’s list and it asked me if I wanted to access location. Many of you with iPhones have noticed how much more we are getting notifications about location used on our phones and whether apps have the appropriate access and the icons will double check if you have the latest iOS. If you are really sure you want google to have access to your location and it gives you this breakdown, using the apple, ones that don't allow at all or allow once and it says they want to use my current location to show me relevant offers in my area. Some of what we learned in this article in the New York times, was that again, some of this data is being used beyond the original intent. It's not just being used and I'm not going to pick on Angie’s list, they are probably wonderful but many of these apps have been providing information to a fairly small subset of companies that follow location data and when it data was provided to the New York times as part of their privacy project they were able to identify a director of a professional committee, a secret service agent, where they lived, where they went, where they were in the pentagon. I have a great example with the CIA. As many of us know the CIA won't even acknowledge most of the time who is an agent or not and yet using this location data it would be very easy to just look at all of those green dots, each of those represent a person in the parking lot at the CIA headquarters where they then leave their phone in the car and figure out that those people work for the CIA. You also have identified people of the senate. People at the supreme court, you had people able to follow the movements of the president. You had a nuclear power station in Florida. All extremely troubling and so I think more in the past couple of years even like a year ago the question was, well I have nothing to hide. And I think this opens up the question, but do we have something we want to protect? Because I don't think any of us want this
information freely available for anyone. And this is also about our kids. So, you have for example, also in this series of articles a device, most likely a child that is track from a home school. They spend the day in this little school in New York and more than forty other devices appeared in school during the day which were then traceable to nearby homes. This of course opens up a question around domestic violence situations where being able to trace back to that location data could be incredibly problematic. In addition to safety concerns there's also issues when this data is used as a commodity. I think everybody in privacy first is interviewed through the story of how targets allegedly exposed a teens pregnancy with the father coming in and saying why are you sending my daughter these adds about formula and vitamins and they came back and said, oh you are right. She is pregnant. I think there are questions about the facts of that case down the road but the thing is we do have habits and indications and big data allows companies to predict things like when we are pregnant before we know and it doesn't necessarily matter if the data is about a particular individual. You had the fitness tracking app which gave people location of secret US army bases because they were pretty remote and the app puts that data online and suddenly you are able to figure out, there's a bunch of people in this remote location. You have photos of your kids. There was an article in the new York time about flick images were used for FACIA l recognition database so data is being used to improve products, sell information in ways that are not transparent and do not build trust and it's between the average consumer, company, government and others. Back to use of beyond original intent: one thing I often hear, and I think it's especially relevant to higher education community is about research and specifically frame researchers from professors who are researchers to others. Well there's never been a data breach of research and research should be trusted. It goes back to that good intent should equal trust, right? And the thing is, it doesn’t, and the reason is you have researchers such as Cambridge example that used data in a way not originally anticipated. The data that Facebook provided wasn't unusual at all for companies at that time and in fact was probably counter to Facebook making more money because the more personal identifiable data they sent elsewhere the less they could use that as proprietary data to target ads and so you had database for research. 2006 AOL released anonymous data, six thousand 50,000 users with their searchers and you can imagine a lot of it was traced back to individuals because the things that we search are identifiable. Netflix did something similar. They released anonymous data that was able to be traced from the movies people had liked and watched compared with the movies that they'd done reviewed on amazon. You had questions about drop box, which shared information, as far as I know it was pretty well anonymous where they shared customer data with scientists in order to further research and there were a lot of questions about well, if this lack of respect for the context of how information was provided is really ethical and you also have researchers that released profiles and that data should be available to the world. Users back in 2016, leaving intact usernames and sexual preferences and all sorts of information that could be used to blackmail and it certainly felt like a privacy violation for any one of those users. When we're talking about research which so many institutions bring into this I think it's really important to consider that when we talk about even big data or data that doesn't necessarily at this moment have to go through an IRB, if you have a lot of violations of basic privacy principles, the underlying framework of all of this is the principles been around since 1970s both U.S. and
Internationally and all of this creates questions about what is ethical and when we're talking about research, even if that research benefits so that counteract this potential privacy violations, the lack of respect for context occurs here. And of course, all of this feels even worse when we get into talking about breeches and bad actors. So you had the very sensitive site, Ashley Madison hack with user dot leaked and we had a lot of sensitive information and the credit reporting agency. I had reporter call me. There were students whose information was posted online as part of open data before a school board meeting. They were releasing their school safety policy and posted it online because the school board was going to look at it and somehow in the layers of review it went through nobody thought to adapt the information about students who would need help in an emergency so it was important that information be there but nobody thought to take to information out of something that they posted online and it wasn't the first year that they had posted this online. The reporter found the student private health information online and that happened to be the year reporter looked at it. Then you also have problems with trolls. People who are in one case a happy group that was trying to troll the FBI, so they hacked into rural districts and higher ed institutions. Phone numbers, texting death threats that pedophiles could shop off of. All sorts of things that underlying trust between the school and the community that terrified people and should down the school district for ten days while they figured out if there was an actual safety threat. All of this lends itself to fear, to wondering how we can trust these entities and you have bad actors potentially using tech in ways never intended. So one thing, one piece of advice that I currently give is think about how your product or the way you are collecting data, how that could be abused. Think of the cases. Think about the LGBT student who isn't out to their parents. Think about someone who is being stalked by their partner or significant other in the past or whatever it may be. Think about that. And think about how the tech or the data that you are collecting could empower those bad actors because certainly you don't mean it that way but that doesn't help as in this new York times story you have certain aspects that can threaten victims. Often allow you to spend your location to a trusted other person. Well what if that person ends up being in a relationship? Is there a way that information could be used to harm students and if so, how do you mitigate those harms? So with all of these front page stories, which I just gave the very smallest flavor, I think it is really normal for students to start thinking about how might this test my school has adopted harm me? It's natural for people to take what they see on the front page of papers, what they see on twitter and apply it to their own context and so how are the students on your campus looking at these stories and the answer is, the large number of reporters who are calling me and being like hey I’m suddenly interested in privacy. Let's talk about how this is used on colleges or how picture recognition applies and all of this. It is utterly understandable that you have students wondering how these things being talked about in the broader policy and privacy conversations, how this applies to their day-to-day lives. You've seen stories just in the past month about colleges at the Washington post appear turning students’ phones into surveillance machines and tracking locations of hundreds of thousands. You have reporting on advocacy campaign which bans facial recognition on college campuses and you also have a recent survey from Educause. I really appreciated the headline here that came out in December where students are not sure if they are invading my privacy or just really interested in me. I think this is a good takeaway for things like
students in programs who are able to likely leverage data for good to evil to provide more personalized intervention and help students get help not just by getting out of their dorm room and walking over to the counseling center, to their advisor but also perhaps in the privacy of their own dorm room. All of that is undermined if students don't feel safe, if they don't feel they can trust you. They don't feel they can trust their institution. So I promised to talk about the most common things happening today and the number one thing is potential legislation, so growing beyond sort of these perception issues that I’ve been talking about, about these long time discrimination power versus people issues. But also about how privacy compliance might change. So privacy in the U.S. has been traditionally regulated through safeguards and law code and arms. Just like anything else. You have broad legal protection against unfair uses of data, usually when a company lies to you, there can be a case brought. The federal trade commission, perhaps by state attorney generals, you have specific laws that provide heightened protection for sensitive information, things like credit scores, health, children's information, your company is adopting technical measures that reduce risk so encryption, hashing, inside scraping policies and then you have social norm that can strain individuals that might use data in un effective ways. For example, that service that I talked about that was exposed fairly recently in the New York times. You ended up with google actually several years ago saying that they wouldn't create that product. You had several companies saying that they wouldn't create that product because they found it so offensive to this sort of creepy notion that they thought that they should not create something that allows you to no longer be anonymous in public. So looking forward, what are we talking about here? So, it's been a little busy just in the past month or so. You've seen the California act and consumer privacy act that passed and went into effect on January 1st. You have Washington state just introducing a potentially competing model that's similar to Europe’s general data protection regulation. You have signs that have come out of Europe. You have a couple major federal bills that are moving forward because companies and congress really don't want to deal with this and want consumers to have to deal with fifty or more laws. Legislators are legislating. Twenty years ago, you had people saying don't do that. You'll interfere with the internet. There will be no newspapers. But today there's a grad student who knows what a cookie is and runs their own server and isn't intimidated to say of course we can regulate code. It seems likely that we're going to be regulating and you see it happening now in states and we're perhaps at the beginning of this federal legislative process. We have the chair, the relevant committees introducing bills both democrat and the republican on the senate side have a bill that's pretty familiar. There's some differences in ideological issues. But who knows? People want to battle. Congress has a pretty busy agenda so who knows what will get through the pipeline in this pre-election year but there is pressure from California where stakeholders are unhappy and that's been the narrative. At the end of the day there are a problem issues with the way it's worded mixed with compliance ripping out their hair but it is very likely that we're going to continue to see models based on California passed around the country and some of this is going to apply to all of you, trickle down to your institutions either through direct legislation but much more often through legislation that's aimed at the companies that you contract with. And the thing is, I want you to keep that in mind but what are we talking about when we talk about privacy law? I'm not going to focus in on this. But this is talking about anatomy of privacy law and the things
involved in all of that, so I'll let you take a look at in your off hours. But at the end of the day, my boss says that technological changes and platform insensitive are going to be a more effective determinant of privacy than law. He brought up in a tweet last year that the changes to browsers, chrome recently announced and others, Firefox, is going to be more to limit tracking than any other legislation. So the things that we're pushing companies into doing is going to have a much bigger effect on what all of you will be able to do and the privacy protections you'll be able to enact most likely than any law that has passed. It's also important to remember that we have more and more privacy risks, things from biometric scanning, social credit and reputation scoring, internet bodies, a lot going forward, new technologies creating privacy challenges and make it easier to take things out of context and use them in ways that are not originally anticipated but this is again something where tech can contribute to privacy as I mentioned earlier and we've seen innovations in technology that are including advanced in identification identity management and advances in ai machine learning that are increasing privacy protection.

So what's your goal? This is an incredibly complicated subject. We created last year that I think outlines there's a lot of risks, there's a lot of sections and your job as a privacy person or just as a person at your institution who is thinking about privacy is to try and bring all of this together to talk about trust, to talk about these power dynamics, to find ways to be more transparent and so when people talk about privacy they feel that they can trust you, that they can trust your institutions. And that things will be -- that their data will be used in a way that respects the context and that will at the end of the day help them and future students. It's important to remember basic privacy principles. Somebody asked about the graphics, yes. There is a downloadable version on our site. This is a great description. I'm a big fan of it and you can all look at that later, but I want to highlight that privacy norms are different in every community. They continually change and are all contextual. Privacy scholar who wrote a bunch about this, it's important to remember that an institution in New York city is going to have a different privacy norm than an institution maybe in a rural community and so this isn't something where it's one size fits all. It's about the questions you ask. It's about how you create the framework that's right for your institution. Essential questions include specifically what questions are you or your institution trying to answer or what problem are you trying to solve? Data shouldn't just be collected. Tests shouldn't be adopted. It should be aimed at a purpose. Where's your community of creepy line? When do things go over what's acceptable to people, to students and you find out by talking to people in your community and getting the student government and others involved as you collect data. What are the privacy risks posed by how you are neglecting or storing or using data and the key benefits, related to that, how can these things be abused? How can these be used to harm certain communities that are more vulnerable? What government structures do you have? What policies? What procedures and then how can you be proactive about public communication and engagement around privacy? Privacy by design is a good way to build this. I won't go through it but it's a useful framework to start thinking about how you can make sure that privacy is decisions made by the various silos in your institution and at the end of the day your most important role beyond creating the policy and everything else that's going to be making people care. How do you do that? Well it's about making privacy important to them. Make it personal. What do the people you serve keep private? Make it about what they care
about whether it's personal politics and beliefs or your institutions reputations ability to be a leader on this issue and this isn't just privacy. It's your whole online and offline, everywhere you are, everything you do, everything you think. Again, it's not really about privacy anymore. And so with that, make sure you engage with amazing research and advocacy. Each of these screen shots are linked and a copy of the presentation that has been shared will be shared after this. Utilizing existing resources, department of ed. Educause has resources specific to higher ed policy as well as general privacy matters that you can use to learn more and implement everything or one of the things I talked about with the underlying goal of creating a culture of privacy. If people don't know why it matters, if they don't know why they care then they'll just go around you. They'll see privacy as an obstacle. It's important from start to finish. With that, we have about nine minutes left and I am happy to answer any questions that any of you may have.

>> Thank you, Amelia. That was great. We have one question from Andy in the chat and he asks, who do you see as simple practical guidelines that can inform practice in legislation?

>> Thank you very much for that question. So, this is something where nobody needs to remake the wheel. We have concrete guidelines from the fair information practice principles that I mentioned to privacy by design principles. You have higher education that Educause higher primers that have 101 guidelines as well as really innovative framework for students' success programs for example where the university of California, and others have come up with guidelines that can be used. When it comes to legislation there's a whole lot of framework there as well and I for lack of time will refer you to the many, many resource areas that are being complied by the international association of privacy professionals that has been put out all over the country.

>> Amelia, you mentioned a couple times privacy norms and I just wondered if you could talk about digital or data ethics in the context of privacy. One of our chief privacy officers, our chair of our cp o group recently shared an article whether you should share about having a digital personal assistant in your home and being present. Just societal norms and privacy, if you could spend a minute or two on that.

>> That's such a great question. One of the things I’ve been working on at more of the k-12 level is training materials because as I mentioned none of this is useful unless people care and to get them to care you have to provide the information and then what information you provide because doing the alphabet soup does not really encourage anyone to listen and so as I said, this is all about making it personal and building it into people's day-to-day lives. So yes, let your inner guts know about your digital personal assistant. I saw a couple of comments that mentioned coming to people's homes when you have dinner parties and try and order lightbulbs or something to see if there's an assistant that's listening to you. But seriously, it is really important to be aware of the thought that as things are more and more connected in our homes and in our lives, the decisions we've made about where we're going to risk potential disclosure of information by having maybe a personal assistant in the home or whatever it may be, those choices may not be the choices that
others want to make and they shouldn't have to waive their privacy rights just by entering the room. So how do we mitigate that and make these conversations something that's happening at the dinner table as opposed to something we're just talking about in the context of this webinar or privacy legislation and I think by each of us taking that extra step, the dinner table or thanksgiving to bring up some of the concerns that happen, some of these stories about privacy that others may have missed. When it comes to ethics, I think all of this is in some way boils down to empathy. It boils down to what should you be doing that respects other people's autonomy, that respects how data can be biased, that respects all these basic things as basic recognition of humanity and the fact that people have a right to fairness. And to having these powered discrepancies addressed in a fairway particularly by their educational institution and so building an apex not only to stand alone but into everything else we do I think is essential.

>> I think we might have time for one more quick question and Amanda asked what advice do you have when trying to explain these concepts around privacy to students and other stakeholders who might not understand the technological in tick assies that cause many of these issues and I had written a similar question around sharing that with leaders and users on campus. Maybe you can try to wrap up and answer that in a minute and half or less.

>> I'll do what I can. It's a big question. It's about making it personal and so that may be providing the slides I just did where I went through all of the oh my god, really? Somebody did that? That's not a great idea. Sometimes it's about just talking about it in a context that they are most familiar with like well, I know you believe this and unfortunately, that was you know distorted when it was communicated in this way and don't you want -- if you were the person who said that on twitter would you want it to be used in that way? Again, bringing it back home to them and how this would interact with their life I think is really key. Personalizing it to a group or to an individual really enables you to provide a peaking experience but again it's not about the tech and it's not about privacy. It's about introducing these concepts to people through stories. And through making them think about other people in those stories and how they would feel if they were the people in those stories. So hopefully that gives you a little bit of something to start with. If anyone didn't have their question answered please feel free to e-mail me or if you want to work with SPS on something we're doing an event before the international oh association of professionals at the summit in Washington D.C. And staff is working on privacy so I would love for any of you to attend this if you are interested or to reach out to both of us. My e-mail is on the screen. So feel free to reach out.

>> On behalf of Educause thank you Amelia, thank you all for joining us today for an engaging session and conversation. Before you all signoff please click the session evaluation link which you'll find in the chat window. Your comments are important to us. The session is recorded, and presentation slides will be posted to the event site. Please feel free to share these with your colleagues. Please join us for the next Educause webinar to hear about building an inclusive workplace session one. On behalf of Educause, this is Brian Kelly. Thanks for joining us today.
[End of Webinar]