Project Completed by:

VZP Digital

EDUCAUSE
Webinar | The Rise of the Chief Privacy Officer (CPO) in Higher Ed
Thursday, January 28, 2021
1:00PM – 2:00PM Eastern
Welcome to today's EDUCAUSE Webinar: The Rise of the Chief Privacy Officer in Higher Ed. This is Brian Kelly, Director of the Cybersecurity Program at EDUCAUSE, and I'll be your moderator for today's event. EDUCAUSE is pleased to welcome today's speakers: Sean Burns, Micki Jernigan, Merritt Neale, and Pegah Parsi. I'll introduce them in just a moment, but first, let me give a brief orientation on our session's learning environment. If you're tweeting, please use the hashtag #EDUCAUSEwebinar. We hope you'll join us in making this session interactive. To open chat, click on the chat icon at the bottom of the presentation window. You can use chat to make comments, share resources, or pose questions to our presenters. Be sure to select “Panelists and Attendees” from the drop-down menu to engage with everyone. We will take Q&A throughout the presentation and we encourage you to type your questions into the Q&A pod throughout the webinar. If you have any technical issues, please direct a private message by selecting “Panelists” in the chat dropdown. The session recording and slides will be archived later today on the EDUCAUSE website. And now, let's turn to today's presentation. The number of chief privacy officers in higher education is on the rise. A recent EDUCAUSE research report, “The Evolving Landscape of Data Privacy in Higher Education,” highlights that many institutions have created privacy offices and CPO positions. Historically privacy was managed in a variety of ways by a variety of roles, including counsel or information security officers. Fueling the need for CPOs are the (sometimes conflicting) requirements of privacy and security and the inability of one role or office to devote sufficient time to both privacy and security. Privacy determines what is to be protected, often including ethical considerations, and provides for the rights of individuals. Uniquely, privacy risk must address risk to individuals and society as well as risks to the organization. This panel will focus on the evolving role of the Chief Privacy Officer. We'll explore recent research findings and hear first hand from current Chief Privacy Officers on challenges and successes. We are delighted to be joined by Sean Burns, Micki Jernigan, Merritt Neale, and Pegah Parsi. Sean Burns is a Corporate Researcher at EDUCAUSE where he provides research resources for EDUCAUSE Corporate Members. Micki Jernigan is the Enterprise Privacy Officer at Augusta University, she is the current co-chair of the EDUCAUSE Chief Privacy Officer Community group and participates in several privacy and security initiatives with EDUCAUSE. Merritt Neale is a Senior Director with Huron Consulting Group in their Higher Education IT Strategy and Operations Group where he leads the group's Information Security, Privacy and Compliance engagements. Pegah Parsi is the campus privacy officer at UC San Diego where she spearheads the privacy and data protection efforts for the research, educational, and service enterprise. Thank you for joining us today. And with that, let's begin. I'll turn it over to Sean and let him give insight into his recent research.

Thanks, Brian. The research project that I'll be talking about today we work with Huron to
develop topics and questions to the higher education community. I conducted interviews and surveys with over 20 private professionals across higher ed institutions and surveys of privacy and decision makers as well. So the next slide I will start talking about how privacies professionals. There is a wide variety of titles out there. Not every institution has a chief privacy officer. There are a lot of areas people are focusing on for privacy. Some are focused on the auditing and security side. And yeah, it has been -- every year I did a little digging into our EDUCAUSE members and we have more and more people with privacy in their titles show up in the years over the last ten years. Kind of the CISO position was ten plus years ago. We are evolving. Yeah, and let me go to the next slide. We can talk a little bit how in the last year, you know we have had the pandemic which has been taking its toll on everyone. Privacy has come to the forefront as people talking about contact tracing, system tracking and any kinds of things privacy is a big concern. But, you know, in the last year EDUCAUSE conducted the student technology survey of 16,000 students and on the right side here you can see this graph that a student reporting they don't really understand how their institutions are using their personal data. I think there is a correlation with the other question, I benefit from the student's collection and use of personal data. Students don't understand how institutions are using student data for a number of programs that aid their students greatly. Especially during the pandemic the need for safety and security of students, faculty and staff on campus. Information needed to be collected. There needs to be trust built up at the institutional level. You can do that by, I hope everyone is focusing on being transparent on the data you are collecting. Transparent about your planning and how data will be collected and how it will used, how it will not be used. Those are the things that have been taking a forefront of interests for privacy professionals this last year. And we can head to the next slide. And as we are thinking about privacy officers have been evolving in the last year, the last years. There are a lot of challenges that people are facing. The number one that was reported to me in my research project was that human resources are really lacking. A lot of institutions don't have a full time privacy officer. A lot of time it is a CISO that has their privacy duties. A lot of those CISOs don't have the time to develop trainings, get involved in the conversation more often. A lot of them could only put 5%, 10% of the time. It is a difficult position and requires a lot of work, time, effort to make sure everything is in order on that side of things. Another one of the big challenges that has really been starting to take the forefront is getting privacy involved in the front end. People are starting to think a little more about privacy. A lot of times administrators and staff won't include privacy as they start discussing a new program. They dump it on the privacy person give us the stamp of approval. It might be late or difficult this 11th hour reviews of any kind of policy documents. So getting involved has been a challenge for privacy officers. And building and deploying privacy awareness campaigns. It is hard to get a campaign together so that everyone thinks about privacy more often and thinks about involving it and including in the early planning and discussions. If we move to the next slide. I want to think about best practices for that privacy officers reported and suggested as they have been evolving in their own positions. As we continue to move through and hopefully beyond the pandemic it is key. It is important to figure out how to spread awareness through conversations across campus. That is just -- it just takes time and takes effort. Sitting down with different departments and talking about privacy and how you can incorporate it into their policy
processes. And as those kinds of conversations are happening. It is important to make sure that privacy -- work hard to change the minds of other institutional members especially like researchers who tend to see privacy professionals in the path in the work they want to get done. Showing how privacy enables everyone to have a better understanding of what privacy means and how it can help students and faculty members just be in a better state. It really helps to improve your position as a privacy professional. Another thing that folks really talking about is working on standardized risk assessments for both new and old privacy offices and higher education. There is a need to conduct -- when people are working with PII and with outside vendors who also require data access to fulfill their services and hopefully Brian is sharing the higher education in chat now. You guys can take a look at that. Vendors can hop on there and fill out their assessments and then they can -- then they can -- any institution can go on and see how their assessment is filled out how they approach data privacy and data security. You don't have to do a different risk assessment at each institution if you do one good risk assessment. Everyone can take a look at it and it is great. Lastly I really want to talk about connecting to the larger privacy community. Having a group like this get together today is just a fantastic opportunity to connect with this community. You know, you can join the education higher education privacy group. There is the invitation chief privacy officer group you can apply. Talk to Brian about that see if you can work your way in there if you are in the position to join that. There is the IPP and other community resources in different states. I know California has a big privacy group for all the state institutions there and they meet and get to talk about the issues they are struggling with and best practices. It is a fantastic community. As we continue to build up around the privacy officer whatever title that takes. It is really beneficial to everyone to continue to build the community and share with each other, share this kind of information with each other. And that will be it for me.

>> Thanks, Sean. I was populating chat with all those resources.

>> Thank you.

>> I can't talk and type. I can type while others are talking. That is a great segue to Micki. We will let Micki go forward with her talk and turn it over to Micki here.

>> Great, thank you Brian and Sean for the great information you have prided today. They were both segues to the things I'm going to speak about today. Happy day to privacy day. Today is the international day dedicated to privacy. Hopefully one day we will get a whole month like cyber does. We will take it for now. One of the first thing I'm going to do, I think Pegah is going to do this as well. It is to describe my journey of being a privacy officer. Long before I knew I wanted to be a privacy officer back when I was in college and graduate school and law school. I knew I wanted to be an attorney. I wanted to work with health care providers and little did I know at the time. There would be a law after I graduated that was called HIPAA. I'm sure all of you heard of that. The HIPAA privacy rule is what pulled me into my first health care role. My first role -- my first ten years in my professional career as a health care compliance and privacy officer. That is a
mouth full. For those of you that are on the sharing this data panel with us today are aware health care compliance should be a standalone job by itself. You throw privacy on because you have this new thing called HIPAA privacy rule. It requires a privacy officer. We add on duties. You will be the privacy officer too. While in health care it is not that much today. A lot of privacy roles. But there is a large movement toward having stand alone privacy officers. Whatever role they might be. It might be a manager level, it might be a VP level. Continuing on my role, the first ten years was in health care. About 11 years ago I transitioned being a privacy officer and a compliance officer in the EDU space. Mostly that was HIPAA privacy with a little bit of emphasizes on FERPA. And then about seven years ago, I transitioned to be just a privacy officer. Now don't let me full you and saying just a privacy officer is not a full time job. That is definitely the role of more than one person. Whether that be more than one person in a privacy office or the various people around campus that you need to help you complete your privacy objectives. This is -- just having a chief privacy officer sometimes is a check the box exercise, unfortunately. When you have a good person in that role who is able to develop relationships across campus then you have champions across campus. It is difficult at time as Sean has said. Privacy is often an afterthought. Especially when people have those personal connections and respect of their colleagues to say should we be using this data in this way? Can we collect it this way? Who can have access to it? Is it ever disclosed outside the organization? All kinds of questions like that involve privacy concerns of that student. Oftentimes our students don't think of it that way until someone points out to them, do you really want everyone to know -- maybe not everyone but administrators to know every time you use your student ID to buy a soda? That's probably not -- beyond a student or a faculty member would expect those card swipes to be used for. They can be helpful in some ways when someone needs to be found or if there is a horrible issue happening on campus and you need to see where people are and get them to safe places. There can be good uses for some of that data. It has to be a very careful and thoughtful conversation and deliberate process to decide how to ever use that data if the occasion happens. One of the things that we are touching on is building awareness of privacy matters and the role of the chief privacy officer or whatever the title may be. It is difficult. It is seen by many which is a perception issue that privacy can be a roadblock. Well, if you bring something to me three days before the contract needs to be signed that you have been working on for eight months diligently the roadblock is not in the privacy office. We could have been working alongside you for the last eight months and provided advice and counsel and you wouldn't need me the last days of the negotiation. The awareness is saying get us on the beginning and we will help you through this and try to answer as many questions that we can anticipate could come if we do this project and we will all be successful. In the U.S., as many of you know, many industries instead of one national law, many industries have a requirement or either strongly recommend having a chief privacy officer. Health care is one, education is
another, financial institutions also have a privacy officer. The difficulty with that as we have seen is all the different competing requirements. And state privacy laws then come into play that aren't typically industry focused and adds another layer at times to those privacy requirements. GDPR or the EU, EAs privacy regulation brought this patch work of U.S. laws into focus for many large companies that do international business. What they saw is wow, this is going to be completely overwhelming and huge finds. If we had one set of rules to follow rather than, you know, 65 or 70, we could probably be more efficient in this space. So hopefully with some initiatives from these large companies and other groups at some point in the near future the U.S. will move to one national privacy law. It will at least be modeled most of us are familiar with it and take the good parts from that and improve on others. At this point we can only be hopeful. GDPR also heighten privacy awareness at EDUs. Many of us especially in the research space -- many EDUs weren't working on focusing on privacy in the research space unless it had to do with health care. They were required to do it for health care. In other areas there were other requirements and limited in scope most of the type. What this required was that the EDUs would do some large scale operation reviews to see where GDPR apply in their operations. And this was helpful. I've been through it a couple of times. It is a great exercise. You always find other things along the way. Even though you are focusing on one regulatory scream you do find other ways. The most impactful thing recently and Sean mentioned this as well is the COVID pandemic. It really has raised awareness of privacy concerns and individual rights. You know, we think of all the things as individuals now not just people working at EDUs it is my information being collected, not just students. It is faculty, it is staff, it is everyone. When they are collecting this sensitive information, do we really know what the purpose is behind it? Is it really to protect me and let me know about contact tracing? Or is there some other use planned for this collection of the data? We don't know at some point. As privacy office see officials we take a step back and try to bring those perspectives when we have them with faculty members, with researchers to make sure any data that is collected is being used appropriately, stored appropriately, accessed appropriately and other things. Retention is a big one that a lot of people haven't put retention policies in place. The people I talked about have been 50/50 on the retention policies. It wasn't the primary focus because we were all, you know, all under complete pressure to try to get things right and do the best we could. We didn't have a playbook to follow. We were all making our own playbook. We did the best we could. Now is the time to ask these questions about the data that has been collecting. I think my time is up.

>> Thanks, Micki. It is a great segue to Pegah. So with that, we will move over to Pegah.

>> Hi, everybody. Good morning or good afternoon wherever you are. Happy data privacy day. It kicks off every year. You will hear lots of different webinars and seminars and workshops and such all month long. If you spend the rest of the year paying attention to privacy maybe take this one month and at least follow along. Welcome. I want to start talking my journey into becoming the campus privacy officer. I graduated law school in the middle of the recession. Things were not going well. No one was hiring for anything especially things like human rights. So I started working in the University setting doing research grants and contracts. I cut my teeth in the
contracting world. And around maybe 2013 or so I started seeing more contract provisions. I could do my due diligence to research the laws and figure things out. I was a little bit limited. Without having privacy office expertise. I don't know, do we have a privacy policy? I had no idea. I started asking questions at the last university. I kept saying what do we do about this? I kept pinging our under resourced privacy office until a developmental assignment came along. I think my boss was tired of me asking all these privacy questions. Why don't you do six months in the privacy office and learn what it is about and bring the knowledge back? The rest was history. I went to the privacy office at Stanford and worked mostly on HIPAA matters around research. But just research matters on international research privacy issues. That's where I learned the day-to-day operations of privacy. Before I came down to UC San Diego to start the program from scratch here. So when I came here I was positioned in an interesting part of the organization which we can get into if anyone is interested. Privacy offices falling in IT, audit or legal. I'm sort of dead center in the university and I have a good wide view of the entire university. That has helped me -- it has its pros and cons. It has helped me move beyond being a compliance person or being viewed as a compliance person or someone that is obstacle and more of a business partner. I kicked off the program here. It is an office of one at the moment for a massive enterprise. You can imagine that would be pretty heavy lift. But in whatever the fate or karma or whatever work I ended up a career that focused on civil liberties and civil rights. Which is exactly what I wanted to do when I went to law school. So things have a funny way of working out. You go off the path for a little while and then you come back. So my passion maybe it is my personal background and how I grew up. I was very privacy protective. As I learned more about the field and the field started becoming more robust and started to expand as Sean and Micki were talking about earlier. I recognized the importance of privacy for our democracy and our society as a whole. I know there are a lot of people that will say you know, who cares about privacy. I'm pretty boring, I don't do anything wrong. You want to look at all my data go ahead, it is boring. I push back a lot on people who say that sort of thing. It is a very limited view what privacy is. It doesn't engage with the parts of privacy having control over yourself. We all know that, you don't have to be a criminal or an interesting person to have privacy interests. Being able to have control of what we do and our data is so important for all of the other values that we have for our society. Things like freedom of speech, freedom of expression, openness and research, freedom and research. Being able to engage with everything around me without fear of either being monitored and nudged or manipulated or monetized or buy things or do different types of things. I truly find that privacy is the next great civil liberty issues for us. And so that is a very long answer to the journey question but I think it is a really important one. It is -- it answers a question that I get often which is why should we care about privacy? What is privacy? Why is it important for our society? So here at the university I saw there was a question in the chat asking about what privacy laws apply to non-profit higher ed in the United States. That's one of the things that I truly, truly love about working in a large research institution. The fact of the matter is that so many different privacy laws apply to us in different ways. Whether it is HIPAA or FERPA that apply to many of the things we do. There is GBLA applies to us, we do background checks on employees. If you are in California we had laws around drones and license plate readers and where they can go and capture. So there a lot of
things we don't think about as higher ed administrators that where the law does in fact apply to us. It just isn't necessary intuitive. We have a lot of laws that apply to us and it is true that many of the ones that grab the headline like the CCPA or the proposition that just passed in California in November certainly those do not cover non-profit educational institutions. But, I think we all - - at least those of us in the business that are paying attention to the way the winds are shifting, I think we all know that privacy is increasingly becoming something that legislatures around the world are taking a look at including for higher ed and research enterprises and what they are doing. This is what I tell my campus all the time. The fact of the matter is you may be able to find a loophole in a current law and hide from it, but another one will coming along eventually. You will have to comply with one one day. So that is how our campus started thinking about our privacy program. It wasn't based on one particular law or even focused on a particular law. It was more about what do all privacy law and our community expectations have in common. Can we start there? One of the first things that we thought about was the fact that almost every privacy law, frankly in security laws start with an understanding that you know what the heck you have and having some sort of asset control. And having asset control, I think is a commonly understood thing. It is not just a privacy matter. How are we storing it? You need it for great many reasons and one of those reasons is privacy. When people say we don't have resources to have a full privacy office or we don't know where to start. I tell them, the first thing that you can do is to start thinking about your processes and documenting what you are doing correctly and what data you are handling. That will get you a significant part of the way in for any privacy law whether it is the GDPR or FERPA or whatever. You still need to know. As they say you can't manage what you continue measure. So starting there if you are low on resources is a good way to go. Sometimes, like I said I'm an office of one. We have a massive university. We have 40,000 or so students. 70,000 employees if I'm not mistaken. It is a lot to do for one person. I had to find my champions around my campus. Those are the people give information to and receive information back from. They help get my eyes and ears where I can't be all the time. Pulling together council the highest levels of leadership to set our institutional, philosophies to guide us, to let us know are we okay to do this or that and let's create some guidelines. That is how I manage the resource issues or I have been for a little while. I know I'm getting to my time but there are other things I want to touch on maybe we get to those in the Q&A though. Actually, let me address this one other question that is in the chat around faculty. It says that the faculty of loss confidence in data security and how do we feel about that whether that is declining or not? I would love to hear what other panelists have to say about this. From my perspective faculty have a back and forth relationship with privacy. I think you can understand that. When it comes, for example, their research or use of student data, they want to have at it. They want me out of the way. They want to go and use the data for whatever they want. When it comes to their own privacy whether or not we are collecting information about employee, faculty, whether or not making them do screenings before they come to campus or making them do, you know tests or vaccinate themselves or what have you, then I'm the first person they call. They call me why is the university doing this with my data? Why is the university doing that with my data? I find there is a love/hate relationship sometimes they have with privacy. I've been successful in convincing many faculty members that privacy is very helpful for their research. Again besides
the asset control question, it helps them down the line. I've seen terrible things go astray just because someone didn't bother get appropriate consent. Four years down the road they had to start from scratch. It was devastating.

>> I think that is great. Another sort of segue to Merritt's wider lens of institutional awareness that lends to some of the questions we are seeing. With that Merritt, over to you.

>> Thank you, Brian. My name is Merritt Neale. My background is across consulting firms. I can honestly say wow, what a different. All the industries I've worked with the only industry when you have a vote and it is 99-1 it is considered a tie. That is indicative of some of the challenges our chief privacy officers are having some of these requirements. Something else I thought was kind of interesting and happy privacy day everyone. Privacy matters complicity. Today's privacy day. Cybersecurity month is in October. We one day for privacy. However, the good news we are also as Micki and Pegah indicated we are definitely seeing some growth in the community privacy or privacy community. I sit in client meetings they recognize the need. There is definitely institutional demand. I have clients have goals and objectives. They are making those early steps. As mentioned earlier those that made those investments are commonly seeing that chief security officer. If the chief private officer is right. We all know that these are two very distinct job functions that sets roles and responsibilities and different ways of supporting the organization. I think another interesting finding recently. We held a webinar on Tuesday. It was entitled security, it is not just an IT problem. Privacy would fall under that as well. It is not just an IT problem. We have five registrants. I think I saw more budget director roles than I did privacy. We saw a couple of the roles as well. It is emerging. It is a small footprint. When we see the organizations that have those Chief Privacy Officer roles a little bit more Pegah scenario we have commitment from some committed partners but we don't have staff. Unlike where we see our Chief Privacy Officer they have more momentum and more staff and have a bit more [indiscernible]. The commitment and the excitement of the things that sustains it. The Chief Privacy Officers are an inspiration to each other. In terms of adopting this as a formal position, I have some clients that have this on their radar. The big piece here is that institutional awareness. Across all of our interviews at the clinical side, college of medicine side, all recognized the need for a privacy role. It is interesting that one of our findings in our survey the other day kind of going back to Micki said about the importance of self-assessments and knowing where you are and what your responsibilities are was very encouraged to see 60% of the people we poll indicated they have conducted a self-assessment in the area of security, privacy, or information related compliance area. Very encouraged to see that. 20% had no plans to do it. Another 20% said they are not going to do it. So still some encouragement there. I think going back to a point Micki brought up that we see that first privacy related role is associated with HIPAA. There is a function in the school that requires that level of position. But I think she indicated it is another hat that someone puts on. Similar scenario they were going to have to fall under -- going through this exercise and benchmark and that role landed with an IT director. Wasn't the best place for that given the roles and responsibilities? We are definitely seeing data privacy is becoming much more visible across the board we are starting to see a lot more security and privacy embedded
with those. Certainly data privacy protection at the top of the list for some of those factors we are seeing there. We are hearing during a client meetings institutions are becoming more cognizant. What we already have with the lack of continuity. Overall we are starting to see that interest come up quite a bit more actually. I know last year we were doing a privacy assessment just touching back on some of the things we have seen. If you are looking for a good place to establish privacy effort, advancement, development, we got a lot of data. I think in those conversations a lot of this is education. A familiarization. I had some heated discussions but passionate discussions in regards the need for policy where the client felt guidelines would be more appropriate. So having those kinds of discussions making sure that everybody understands what these terms are. That push back and those challenges along that line of policies required was the institutional line of thinking as well. Just a couple of final thoughts I wanted to wrap up. I thought it was this morning I attended an orientation for a program at the university related to cybersecurity. Closer to the end of the session somebody asked will this available online or something we have access to? The professor indicated he was responsible for editing that content. He had to follow-up with the students. So very much a different line of thinking than what we see in the United States to some degree. I think that drives back to what Micki and Pegah were trying to drive home. This does require policy. This requires education, collaboration, and enhanced communication. This requires a dedicated professional leading this charge. It takes commitment of time, resource, energy. It is more one person can do. I think that pretty much sums up. This has been a great conversation. We have some questions here in the audience.

>> It has been a great conversation. With that Sean Burns did had to drop early. We will make sure he will get his contact info for anyone who wants to reach out to Sean directly. We have about eight questions in Q&A. I think Merritt, Pegah and Micki. If you want to chime in and jump in on some. We will take that approach. If that works?

>> I can take the one about the third party providers. This is definitely something that has come up more and more is around really understanding the practices of our providers. And in some cases running them through a process of understanding what practices they have in place, what kind of training they have for their employees, what kind of safeguards they have in place and understanding what the best practices are that are implemented. I will say from a standpoint we see this emerging quite a bit more. Privacy and security are getting into these contracts and into this cycle to evaluate the risk associated with our vendors. Some are comedies service and some are proving critical services we need to safeguard.

>> Thanks. I was talking. I think I might have cleared a question accidentally. I apologize that for Micki.

>> There were a couple that I selected I would answer live. One of them. Forgive me I can't remember all of them at this moment. One was about the coordination with the university librarians because they have been responsible for and attune to privacy matters for many years. I
absolutely agree with that. I haven't had the opportunity with my new organization and COVID has dominated our landscape for so long. At my former institution we did work very closely with administrative officials in the libraries to sometimes begin conversations for our campus to say there are things going on. Can we model what has been done at the library for any reason? Taking inventory. We were able to take inventory of policies or procedures or things they were doing that we may be able to model in other areas. I say yes reaching out to the university librarian or staff is good idea from a privacy perspective.

>> I was looking at the question around the trend to combine CISO and -- compliance around privacy. I can find that link where you sort of answer that question.

>> I am finding just antidote tally they are being separated as opposed to one umbrella. I think Huron and EDUCAUSE have done scientific research.

>> I think you are right. If it is recognized it is combined with the CISO. Then there is next evolution of breaking it apart. That is the forecast that this role will be separated and the CPO will be the recognized important role within organizations which we agree and concur wholeheartedly.

>> I agree with that in that the needs of a privacy officer versus the needs of a security officer and the roles they play sometimes conflict. There needs to be two voices in that space instead of one individual for which that person personally feels what is right for privacy versus what is right for security.

>> I'm scrolling down how much time are you spending on privacy ethics issues in AI and facial recognitions. Does anyone want to comment or chime in on that?

>> How much time?

>> Go ahead.

>> Go ahead.

>> I would say before the pandemic began there was a strong push toward recognizing putting appropriate policies in place including Pegah mentioned about license plates readers. That is another area think about that being a privacy conversation. After pandemic hit --

>> We got about five minutes left. This is one of my favorite things. In cybersecurity and sometimes in privacy we always sort of focus on where we are losing. We don't always talk about where we are winning. There is a question sharing your privacy success stories. Maybe you can close with a success and how we won the battle.
>> Who wants to go?

>> I can start. I'm doing some work now in the security assessment with a client. I think throughout the life cycle of our conversations I was encouraged to the fact that faculty, staff, researchers, administrative staff were all aware of a privacy need. They couldn't necessarily articulate it. They knew there was a need. They recognized that they had a HIPAA privacy officer but that person wasn't necessary the best suited for a cross enterprise role. For me it has been encouraging this evolution and the awareness raised. I think I'm seeing that in the universal level. There is push back in some spots. I think finding those champions and stakeholders you can engage with is a critical move shifting the immediate.

>> I'll give an example of a concrete thing from last year. So we have our campus a pretty extensive return to learn program that include all sorts of things. Weekly requiring testing for our currently on campus working students. Daily system screens and now vaccinations. There was one part of that would have been either a fiasco if we not had a privacy conversation. We don't need to go into the details of what was happening. We needed to balance the idea we needed as many people to participate in a particular part of a program as possible and yet forcing everyone to participate would have caused a huge backlash. We needed to find a way to allow people to opt out of the program. The people that wanted to. And so we had a conversation with those people and those that were dead set on being opted out were able to opt out and everybody else was opted in. Because we were able to have those conversations at the highest levels with the chancellor, with our CFO with our health professionals we were able to launch program and have a successful return in fall. A good privacy win. There are lots more but that was one from last year.

>> Micki one for the win?

>> Mine is similar to Pegah's. Privacy was asked the right questions about collection of data on faculty, staff, and students that was not privately collected. Was not going to have consent involved. We were brought to the table and listened to. It was a big win because the data was never collected. There was really never no use for the data. People were thinking of collect the data but they weren't going to do much with it. We got to the point not necessary a privacy concern it is an ethical concern. Why would you collect this sensitive information on these individuals if you don't have a reason to use it? We were heard. So that was a big win for the privacy office too.

>> Awesome that is a great way to finish right on time.

>> On behalf of EDUCAUSE and our speakers, this is Brian Kelly, and I thank all of you for joining us today for an engaging session and conversation. Before you sign off today, please click on the session evaluation link—which you will find in the chat window. Your comments are very important to us. The session's recording and presentation slides will be posted to the
event site. Please feel free to share these resources with your colleagues. If you enjoyed the content of today's event, we welcome you to join the first installment of EDUCAUSE's new thematic series that spotlights the most urgent issues in higher education. We're starting off with “Post-Pandemic Future: Implications for Privacy” launching on February 15th. On behalf of EDUCAUSE, this is Brian Kelly, thanks for joining us for today's EDUCAUSE webinar.