Project Completed by:

EDUCAUSE
Industry and Campus Webinar
Data Privacy Panel Discussion
Tuesday, January 26, 2021
1:00PM – 2:00PM Eastern
>> Welcome to today's Industry and Campus Webinar: Data Privacy Panel Discussion. This is Jason Martin, an Online Event Producer at EDUCAUSE and I'll be your moderator for today. EDUCAUSE is pleased to welcome today's speaker: Christian Auty, Ben Nixon, and Nicholas Pidek. I will introduce them in just a moment, but first let me give a brief orientation on our Session's learning environment. To open the chat, click on the chat icon at the bottom of the presentation window. You can use the chat to make comments, share resources, or to pose questions to our presenters. Be sure to Select “Panelists and Attendees” from the drop down menu to engage with everyone. We will Hold Q&A until the end of the presentation; but we encourage you to type your questions into the chat 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. Meeting data privacy compliance isn't always as Pretty and neat as the regulators think. Today we will have a panel discussion about how to “win ugly” when it comes to compliance. We'll discuss GLBA, FERPA, HIPAA, and other Regulations and showcase real-world examples from legal and higher education perspectives. Christian Auty is an experienced adviser in a wide range of data privacy and security matters. Christian has helped hundreds of companies in diverse industries navigate complex data privacy and security regimes, including the California Consumer Privacy Act, the GDPR, HIPAA and the Gramm-Leach-Bliley Act. Ben Nixon is the Director of Information Security at Point Loma Nazarene University. With 20 plus years of experience, Ben is a skilled communicator and strategic thinker and is a leader in Information Security for Higher Education. Nicholas Pidek is an entrepreneur, business consultant, and the Chief Marketing Officer at BitLyft Cybersecurity. Pidek graduated from Kettering University and has a background in B2C, B2B, and bridging the gap between the engineering and marketing mindset. And with that, let's begin today's Industry and Campus webinar: Data Privacy Panel Discussion.

>> Thanks so much, Jason. I appreciate that. I will do a quick intro of sponsors a little bit about me and BitLyft and we will get right into the speakers. I know you are here to hear them. We exist to eliminate cyber threats. Looking to overcome some of the security shortage with the talent obtaining that talent, getting that talent on your team and utilizing the best technology we
do that through services and MDR. You can look us up at BitLyft.com. One of our sponsors today is secure onyx. We implement them in our platform for our secure posture. I'm going to kick it off with Ben and Christian. The first thing I want to outline. Why did we use the term knowledge win ugly. This is something that, I think most people in the info sec or data privacy in the security tool realm it is fully integrated and does all these things. You talk to people like Ben and talk to people like Christian it is really messy to implement some of the policies and compliance. It is not easy. We wanted to get real firsthand experience from what is happening from a university level. What is happening from a legal perspective as it relates to data privacy? With that Christian and Ben thank you for joining me here today. I appreciate you guys being on.

>> Thanks for having me.

>> Ben, I'll start with you today. Tell us a little bit what is data privacy mean to you in the into sec and higher ed? What keeps you up at night? What wakes you up in the morning?

>> I'm responsible for the information security at the institution. Looking forward making sure we are in compliance before we need to be. My team is responsible for the cybersecurity side of the institution. We are implementing the technical safeguards to do so.

>> Christian you have an impressive resume. How do you interact with this on a day-to-day basis?

>> You know what for me what I really enjoy when I'm working with my clients. We have oftentimes clients are consulting multiple regimes and having to do that in realtime. And so what I pry myself in doing what excites me is bringing a mindset to the advice we give and to make sure you are not only being compliance but getting the most data in any way possible.

>> That's great. Ben, coming back to this win ugly terminology. 2020 was an insane year navigating unknown. Most of the world dealing with this. But what does 2020 look like for you? When we were talking with people last year in August, people were kind of wondering when kids are coming back to school. What will it be like? Are you feeling a relief from that? Do you have new challenges ahead of you? Where are we at now coming into February where you are at with the post dealing COVID and how you see the future moving forward?

>> We have found our footing from the changes. They are monumental shifts. They work from home. Looking forward I am anticipating -- the solar winds attack highlights the need continuing to assists with their parties what data you are giving them. What level of -- they may have to your institution or network? I expect that to be a lightning rod this year for my institution. We have seen an increase request documentation of those third parties assessments being done. I'm anticipating a more robust insurance. We have an established support group where I am based. I'm hearing from my fellow colleagues that the insurance renewal process in documentation needed before the entrance renewal completed.
That's great. We were talking offline before this got started. I asked you what is something that has been shocking in your world or interesting. From your standpoint what are you seeing changing in data privacy. There has been big shifts from last year to this year. What kind of keeps you up at night? What are your clients coming to you and asking you to help them figure out.

What keeps me up at night is what am I missing. So many things have happened in just the last year whether we are talking about -- the real attack from the EU to the United States. Whether we are talking CCPA which has come into effect. Whether we are talking about breaches, solar winds what have you. Whether we are talking about management. I agree completely with Ben. It is going to be a big issue from a regulator standpoint. They are going to see, other regulators are focusing on manage. It is somewhat new in a lot of ways. It is a piece of change in 2020 was really in order of magnitude higher than we have seen previously.

You mentioned the term topology the unspoken cousin that no one wants to talk about. We are talking win ugly. Black bod can you walk us through. You want to protect your organization and how you are dealing with it not put too much out there. You shared that with me. Do you want to walk through what has your university your view with interacting the clean up from black bod. We were impacted by that incident clearly. It was an eye opener for my institution. We had not had something of that impact hit us. It was interesting to see the communications happening and the discussions around that. Certainly highlighted our need for a more robust response plan and who makes calls of what to say to who. When do we initiate with legal conversations like that. Looking forward, I think it is really have been an opportunity for us to demonstrate and improve back to the vender management that process to make sure we have the right controls in place and we are properly assessing. Understand where that data is going. What data is going out is key to being able to correct it better.

Do you feel like you have a good pulse with vendors? Say like hey, I want to clearly every aspect what you are doing from my data from you as a customer perspective? Are you engaging that? How do you deal with that?

It varies. I dealt with a vendor. They gave me more information than I needed. Last one I did one and they didn't want to talk to me at all. If you do it on renewal of contract they are much more likely to participate in that. We use higher education vendor assessment tool. They can provide it to others. So we leverage that first. At the same time we have to take supplemental information because they refuse to play ball at all.

And this is something too. I'll ask you Ben but Christian I'm sure you can weigh in on this. You mentioned to with me in the aftermath one of the things that came out and you had to go through is the different states of different requirements. You are based in California. We will get into the CCPA and what that means for the future of higher ed. Can you talk through that what
you experienced with these different states if you are dealing with students that are coming from New York or Michigan or got your residents? How do you navigate between states and what the states requirements in data protection?

>> We had 18 states that were impacted by our incident with black bod. It came down to understanding what each state requires. Given the combination of data that was exposed. Our data set was different than any other institutions. Our answer in the state of Washington than theirs in response. We had to rely heavily on our office. That is a great hand over to Christian just understanding those complexities and being are paired for them.

>> There is 50 state data breach laws. Each one is different. They have their own flavor. There is a little bit of playbook to this when you have gone through much brief responses. You start to get kind of familiarity with the state law requirements. You know, an actual privacy law. What I mean by privacy law like a you are having to address how you are dealing with data every day. What are you doing with it? 50 state data breach laws is unworkable but not unworkable. And, you know, you are in a situation where they are legislative for the entire country. I think we can expect that to change. But I would like to see a federal preemptive law to bring this all together so there is one law they follow. Hopefully they tackle data breach so we are not dealing with separate notice requirements. And we are not dealing with different triggers. But, you know, it remains to be seen.

>> I second the federal guidance.

>> If you will ask Google and Facebook they would have said absolutely not. You ask them now. They would say yeah, I want one.

>> You mentioned the California Consumer Privacy Act. You mentioned in the for-profit world. What is happening from legislative or lobbying standpoint as regards to CCPA?

>> CCPA draws the line around consumers. The valid initiative depending on what provisions we are talking about. I think -- it is more likely to be a federal law. GDPR obviously applies. What regulators will eventually grab hold of. We are really interested in consumer. We are interested in data subjects. In order to do that and especially in order to protect the sensitive data we need to apply it to non-profits as well. I expect regulators to take that step. I don't know that is the right step.

>> That's great. I just saw this come through from Mike. He asked about CCPA. Is CCPA applying to sharing of information? Could you unpack a little bit? Just briefly for Mike there.

>> CCPA applies to make 50% of revenue from sharing of data. GDP regulates you have to have a reason, tell me why you have the data. What is your reason for having this? CCPA regulates by restricting or conditioning the sharing of data between entities. You have to have some contracts
with your service providers. It does this with the concept of selling. Is a -- is the concept when you deal with selling of data.

>> Thank you for that. I appreciate it. So this question is going back to you Christian. You know something that we have seen from our end and talking with other higher education institutions. This is happening outside this industry as well is the transition to the cloud. The infrastructure that is there. We have seen a massive shift in navigating from home environment in this move to the cloud. What can be done from a legal standpoint as we add more of these services? Ben talked about vendor management. There is efficiency come with the vendor. I can sign up and my ERP is taken care of. My fund-raising and collection of that is taken care of. What can we do to bolster the terms? They can say these are -- our new TOC's and what organizations like Bens or other organizations do to protect themselves from that as this move to the cloud is happening more and more with vendors and maybe not necessary knowing what is behind the scenes but what vendors are doing with that data.

>> I think I break it into three categories. Let's break the vendors. There are really three basic categories. First category is your massive players. Your Googles, your AWD, your Amazons. Those guys are not going to negotiate with you. If you want to work with them this is the circumstances under which provide you with cloud services. This is the circumstances which we provide you with business associated agreement. Very rarely will they modify those terms. What you are getting there you are getting top of the line security. You are getting everything you could want from a security standpoint. You are at the top of everything. Second bucket is the folks that you can work with your paper. You work with your council. Get an understanding of what you need. Understand what security you need from vendors. Have that template form in place. Go and understand what we will and will not accept as an organization. Have your paper and have them sign if you can your paper. It will do all of these things that are going to allow you to go back and make sure you have the security and you have the stipulations that you need. That's the second category. The third most dangerous categories which is the folks insist on using their paper. But that paper -- there maybe not at the very, very highest level. That's where you have to dig in with council. Make sure you are comfortable with the security that is being promised in the agreement. And make sure you are comfortable with all those other things. You are the one that is going to have to answer the questions from the regulator. You will have to do the breach notifications. You got to make sure you are protected from that standpoint. What do you look for in these agreements? You want to make sure it is insured. You want to make sure the security is meeting the needs of the regime that you have to meet. You want to make sure the security is good enough that you are going to be comfortable sending your data over. You want to look for overpromises. If someone is willing to sign anything and is not modifying agreements not engaging in discussions. It is saying -- you really want to take a hard look at something like that. Is this person just signing this? Are they actually able to meet all of the stipulations in the agreement?

>> Ben, this question is for you. You are dealing with data privacy. You are dealing with GLBA.
From your perspective, what do you see will be the most challenging to address in this year or in the coming years ahead from what you are seeing coming from a legal standpoint but more specifically just your perspective. What do you see as those hurdles you are trying to check off or get ahead of that you have to address?

>> Well we have mentioned the different state data breach laws. I think we have 28 or 20 something -- I should know that better. We have constituents. And understanding what we have of data for each of those states. And the other thing, I know there are proposed changes. I know they are coming. Do you have any update on that? Any progress or expected timeline or when the changes may be implemented.

>> I know the comments were due in August. I don't have an update for you on that. I completely agree with the underlying premise. What we are going to see is more specificity with respect to, you know, regulations imposing actual specific requirements like for example New York DPS which is a law. You must have multi-factor et cetera. You are seeing that now from regulators. Aside from a couple of exceptions. There was not the specificity. There was this general I want you to go out there and be reasonable. Article 32 just be reasonable. We are going to Monday morning quarterback you after. You had a breach. Obviously you weren't reasonable. Now what we are seeing in terms of maybe, FTC updates make in terms of some of these new safe harbor. Now what we are seeing more specificity. If you can meet those perimeters you might be able to say I met those perimeters that is a reasonableness standard. And they are for, you know, I shouldn't be fined. I wasn't neglect, I shouldn't be sued. I think that is the term insecurity. To a large degree around the fundamental and basic structure of GDPR around the world. Not just in the United States which CPRA what this new ballot initiative moves CPRA. Like was in Brazil, like wise in India. They're adopting this control processor. They are adopting concepts of sensitive data. What we are seeing the original script in the data privacy world.

>> So could you talk to more too for those who are on that are watching that are in higher ed e that may have focus on GDPR comes into play. Maybe this is a good segue. You kind of give a short intro to what are the things we should be conscious of. The three things you should be thinking about and segue what can organizations in general do to set themes up what is happening in that regard.

>> Sure. Hopefully had the GDPR conversation. Does this apply to me? Given what I'm currently doing. The real question am I doing enough in the jurisdiction to, you know warrant application of the law to me. Such that I'm going to go through this compliance exercise. That can change. It depends how active you are. Obviously beyond the scope. Does this apply to me? If I determined it hasn't do I need to revisit. Had a lot to say territorial application of the law. That's the first thing. The second thing, you know, so I'm thinking about that. I'm thinking about if the law applies to me or I'm working with folks. I'm thinking about cross board data more than ever. That's probably the biggest decision, the biggest lightning bolt of the year. So everybody who went through the privacy shield program, right? Which is Department of Commerce
program. And what the justice said we are going to much, much, much scrutinize the flow of
data to the United States in particular from Europe and we will encourage where there is one for
each country we are going to ask them to scrutinize data flow much more in the United States.
This is something, you know, the old rules no longer apply here. We are not -- we are not sure
what the new rules are. The big takeaway is the flow of data from the EU to the United States is
under attack like never before. There will be a political solution before there is a legal one in my
opinion.

>> Thank you for that. I know there is a lot to unpack there. There is plenty to read on. I want to
shift a little bit and kind of go to PII and talk about when is the collection of user too simple to
identify a person. What I mean by that, I'm sure you are both aware there was this -- there was
this ploy from the credit cards. You don't know who these people are. With enough data points
they begin to be able to discover I can find out who this person is. And as it relates to higher
education. As it relates to not necessarily institution but the students or users interacting with
institutions with the Facebook or Google. When is the collection of user data in a school
environment too simple to identify a person? Is that a conversation you are having been at your
institution how do we really not grab so much information about everybody as much as we can
and hold on to it. What is the liability in holding that information? I have one caveat to that. With
the introduction big movement in AI and all of that data to get more meaning out of it. What is
that exposing institutions or organizations as they are trying to get all of that data. It runs off
data, data, data in the security realm we will only want the data we need. I'm unpacking a large
topic. If you want to talk about your institution thinks about that. Christian I will love to hear
from a legal perspective.

>> That is a conversation allowed for me to have those conversations. It works people up. Do we
need to store all the data we have for all of constituents? So we are working towards data
minimumization. One thing I am congress that sent of the definition is continuing changing. The
data is -- dictates that from state to state or country to country. Trying to stay on top of that. The
combination we may store over on a platform may not be considered PII today but might be
tomorrow. Are you auditing, are you tracking, are you making sure you know the data?

>> Christian, what about with you? What do you see from a legal perspective?

>> We were talking about CCPA. There was amendment to CCPA. Specifically with respect to
health data that imposing a contracting standard on non-profits in California. You just reminded
me of that. That is what we are talking about. We are talking about one document retention and
data retention. I want my clients to be thinking about. Do we need to collect this and how do we
get rid of it if we don't. Once they realize the data presents more of a risk than it does a benefit
not always the case. Very frequently the case. They start looking what is the best way to do this.
Sometimes it is to delete it and sometimes to be identified. It can be useful later in other
circumstances. The way I think about identification I think of it get out of jail free card. If I don't
want to deal with HIPAA I identify under the safe harbor. If I don't want to deal with GLBA ID
identify under that particular regime. Same for CCPA. GDPR anonymization. There is a -- it is truly value in a lot of different ways to the organization in terms of, you know, using data in a responsible manner and removing it outside of these regimes. I think we will see a lot more identification. A solution for a lot more problem sets. Including AI. You got many learning and issues around profile. These things are automatic decision making. These things are address in GDPR. So starting to dip their finger and have jurisdiction here. But we haven't seen the concern at European level in the United States yet. Like I said, I definitely think there will be more of that.

>> As regards to that and maybe this touches on GDPR more specifically. When there is a request for deleting data. A user wants to take control of data about them. How do you delete the data? How do you prove that in a court of law if somebody were to challenge that?

>> I don't know you would -- first of all, maybe -- you would not have private right of action. The only one available is for data breach. You will have to prove it to the regulator. What CCPA you are supposed to keep a log of the requests. You are still processing certain pieces of personal information. When I communicate with a CCP data subject. Your information has been deleted we are keeping this one piece to prove that we did it. You are going to be and you are just are. Under GDPR there is no obligation to do so. There is some kind of morph language which allows for full and complete deletion. You can say I can't identify you because I deleted all your data. So that's kind of a long winded way to stay you can kind of keep a record of it. The fact that you did it. But, you know, more to the point certainly under CCPA very frequently clients are finding there is a requirement lesson than under GDPR. It is not as big a problem as you might imagine.

>> Thank you.

>> One conversation that we are having at my institution. As we anticipate eventually apply some form of CCPA. There are certain types of data we can't delete. Whether it is financial aid. We can't delete all data. That's another conversation that needs to be had as well. Hopefully can be included what it looks like to give some guidance there.

>> Just saw this question come in. It unpacks and maybe shed a different angle. The question is what recommendation from handling the higher ed argument for use in continuous improvement that you are imposing business rules and form institution. Either one of you guys want to grab hold of that one?

>> I think it is a risk analysis. If you need the data for a business purpose, keep it. Let's protect it properly. If you don't need and can't justify the continued tension then get rid of it.

>> I completely agree. This is why retention programs are so difficult. It is different for every organization. Some person's treasures are another person's trash. It is a conversation that requires
-- this is what I enjoy most of my job. It requires buying from a whole bunch of constituents. It is not just research. You got to get everybody to the table and have that conversation so you know where to go when it comes time to justify or delete a particular data.

>> That is a great point. It has been more of a faculty perspective. It looks like identifying might be an option. Where do you start with training people how to do that with data that comes from a learning management system? Either one of you want to respond to that?

>> I think it comes back if the data is needed for educational purpose maybe to be able to argue later or verify they met a course. Then you need to keep it. I don't have --

>> It makes sense to me. When I talk about identification what I'm talking about is much more of from a holistic perspective. You got this huge set of data that you determine you no longer need. Maybe think about deleting and identifying it in case there is something you want in the future. It is by definition personally identifiable. So, I'm looking at this. I'm looking as a solution in thing aggregate. It tough to tell a faculty member you got to get rid of all of this information especially personal -- we talked about this earlier. Personal identifiable information is not a straight forward analysis. There are people doing nothing but -- it is statistical and this other stuff. Getting to an identifiable individual with an address and zip code might actually be possible in some scenarios. So to have one individual be tasks with doing that with respect to any particular data set.

>> That's great. I appreciate that response. I got another question. I'm going into some of the audience. I want to make sure we include that. This is about PII. Can you speak to PII and the inclusion of stay tuned IDs being categorized as such.

>> Again to bring it back to black box, we try not to. That is one thing we learned there were two states with a certain combination we had with the student ID it was reportable set of data that required notice.

>> Yeah. We should draw a distinction between PII and a trigger report. So PII is my name. My email. If you lose my name in a data breach. I'm not going -- you don't have an obligation to report in my state. It is the name plus something else. A name plus a password. It is a name plus a credit card. A particular kind of identifiable information that is going to trigger the notification obligation. That is in the United States. In Europe it can be anything can trigger a notification.

>> This is another question going off from that from PII. What about location data? If universities are using that to track movement and track location. How does that fall into that category of what is protected and what do people need to know about that.

>> Go ahead, Ben.

>> We don't collect that. I can't help you there.
So location data is -- let's talk about different species of location data. If I was just to say Texas. That is not identifiable information. It has to device, ID. Now I got something that can be related back to an individual. There are other kinds of sub parts of location data that present a lot more interesting issues. Internet protocol addresses. This is a huge deal for a lot of folks that are in the Internet. Folks that are relying on web pages. In some context you are argue that IP address is not personal information. The IP address if your public address. Your IP address at home could be just you. And CCPA modified the personal information to include households. I believe they did so because they didn't want to deal with the arguments an IP address is never personal information unless the single individual is living home alone because it could be one or more member of the household. This is to say there are a lot of nuance and how it gets triggered.

That's great. Thanks. I know there is lots of multiple definitions and who is looking into it and who is defining it and who has the stick to actually define it further. Another one of the questions here. I do want to open this up we had some organic questions go back and forth. Ben you can feel free to ask Christian some questions and Christian vice versa. This is coming back to the different states. The previous questions. Why do you not go to the most stringent version?

I'll start. Operationally we do. When it comes to reporting, I think it comes back to a business decision. That's what we saw. We have seen most recently. Do you want to report to all states in the same way you are reporting? You may only have to report a few dozen individuals. Christian, I'll let you handle it from there.

I agree. You will have to find operation a common denominator. The reason you got to deal it differently from a reporting and breach notification states are specific in how you report. Some require you to list the number -- the estimate number requires that you don't. So you got to get really state specific in terms of the content you are pushing out to individuals or to the media or to, you know everyone essentially. It is a question of complying with different state by state mandates in the breach notification law.

Thanks for that. This is a question that came out. This is from Jonathan. It says love to know how in other institutions deal with MLS integration. I've been struggling with reviewing our contract vendors. Publisher innovations paid by the students or textbook adoption.

We take a look at those. We are struggling with the same thing. We struggle with that as well. We take a look at it in -- is this going to get access to the organization dataset or to the individual student. On the student level we let them do it if they choose to. We provide some guidance depending what guidance the app is asking for. If it is an institution level access. We have had to say no a few times. If we have to come and say no we find an alternative that meets the need.

That's great. There is one other question here I wanted to get to. This is from I guess I don't know the context of this. So Christian, one of the things to come back to anything else that we
should be made aware of? I know something you are personally passionate about. Is there anything you can say or a couple of key takeaways we should be thinking about as it relates?

>> The first thing if you are relying on privacy shield. You got to get that out of there. There are a couple of different ways to do it. The second thing if you were relying on privacy you probably not signing clauses. Now you have to. And you might have to add to that. You might have to develop a law enforcement policy and other policies in order to comply with the letter and spirit. You know, it is essentially -- it is a repapering exercise. Over the top of the paper exercise that you did in 2018. You got to do it again. The thing I want you to think about when is an organization should we do this? We are out of compliance right now. We know that there is going to be updating standard clauses. There may be an updated in place. There is going to be a lot of development. You don't want to be reaching out to the same vendors. It is not manageable. That is not manageable or from a band width standpoint. I'm afraid, it is difficult to be more specific than that until you get to working with the actual --

>> I have a question for you.

>> Go ahead.

>> Michael alluded to this earlier. When it comes to the requested to delete data. Did any of the laws provide any guidance on validating or verifying that identity? Is there a benchmark making sure it is Nicholas before you take action?

>> There is. Especially important. In is a lot. So less just talk about CCPA. There is a lot around validation of individuals and authorize agents in the CCP regulations. They are kind of obsessed with this idea. This is very specific examples of how you verify an individual identity. There are different levels depending on the type of request. So the right to access request would require more verification. More validation than a right to delete. And then there is this concept of very scary concept in my view of an otherwise agent which is somebody that request on your behalf. This was the sort of the future of consumer vindication. Kind of a class of consumers in multiple organizations at the same time. There is a lot. There is a lot to verification primarily on the CCPA side of things. My advice on this you got to look at what data you have and craft a verification methodology. It just clearly depends on the data set. You can't -- there is no one size fits all. How do you verify. Depends on what data you have. We can't verify you. This is a perfectly answer if you can defend it.

>> Good to know. We are seven minute out. I want to transition to you if you are watching. If you have any additional questions throw those in the chat box and put the panel list and attendees so we can see that. I want to put it back over to you Ben and Christian. Any final thoughts and takeaways. I know we talked about different topics. Are there takeaways or things you want to charge your peers as they transition here?
I would say there is a lot of it happening in the chat. There are a lot of resources. There is a lot of great information out there. Resources. Seek them from your colleagues. I've been able to accomplish a lot with the resources are there ready to be used.

Christian, how about from you?

Absolutely. And look -- I think the big tea here is that there is a lot going on and this can feel really complex. If you have certain core key principles. If you attack certain principles and issues directly and do it the right way the first time. This greatly and dramatically simplifies it. If you do a good data inventory request for deletion is a lot easier. That sort of stuff can be valuable to the organization. Even as you are sort of checking boxes and complying with regime, now I got to deal with this. There are ways to do this that are not painless but relatively pain free and still provide great value to the organization. That's great. I appreciate that very much. Anything else before we wrap up here? I probably made everybody's screen go full screen as I share screen. I want to --

Hit escape. We learned that here.

I put this back up here for Ben, Christian, or myself if you want to get in contact for follow-up questions. There is our contact questions. Any other closing thoughts before we wrap up here?

Thank you for the opportunity and thank you for moderating Nicholas. You did a great job.

I appreciate your time. Thank you EDUCAUSE. Jason anything to wrap up here.

The sessions recording and the presentation slides will be posted later today. Please join us for the next industry and campus webinar on January 28th at 1:00 p.m. eastern to hear about the rise of chief privacy officer on higher ed. Thank you for joining us today.

Thanks, everyone.