Afternoon, everyone. You’re listening to another Educause Live. I’m Mark Hoyt, Vice Chancellor and CIO at Tennessee State University. Educause Live webinars are supported by Dell, and to check out more about Dell and the support for higher education, please go to dell.com/highed.

You’re probably familiar with the interface at this point for our webcasts, but I want to make sure to encourage you to make these sessions as interactive as we can. On the left side of your screen is the Chat window where you can submit questions for speakers, share resources, comments, and chat with each other about the issues going on in the Chat in the webinar. And also there is Technical Help right next to that window if you have any problems. Hover over that and go ahead and send a note to Technical Help if you’ve got problems.

We also monitor the Twitterverse, and if you use the hashtag pound edulive, that’s E – D – U – L – I – V – E, we’ll follow that and add those questions in.

This session, like all sessions, are recorded, so you’ll be able to get the recording, the slides, and archived on the Educause Live website.

If you should experience any audio issues, please check the audio link the lower right-hand corner and send some technical help through the Chat window.

So let’s turn to today’s webinar. I’d like to thank you for joining us and keeping (inaudible). Robert, you might be making some noise there. Today we will take a deep dive and explore our right to privacy. I must confess the title of this session, Location, Location, Location, was intriguing to me in light of the recent public debate and the probe of the National Security Agency’s massive data collection program. Why is our presenter focused on data rather than content? Stay tuned and I think he’ll make it clear.

In the next hour you will be able to click the reset button regarding the way you think about privacy and your right to it.

Before we begin let me introduce our presenter. Robert Ellis Smith is an expert in all aspects of privacy in the United States, including internet privacy, computer security, electronic surveillance, social media, and the constitutional right to privacy. Besides being the founder and publisher of the Privacy Journal, Robert is also an experienced journalist, lawyer and professor, as well as an author of several essential books on privacy. Robert has been asked twice to write the definition of privacy for the World Book Encyclopedia. Please welcome Robert to Educause Live. We’re pleased to have you here, Robert, and take it away.

Good afternoon, Mark. This week represents Data Privacy Day, which began about five years ago, and I think the most appropriate way to mark it is to try to update our skills with regard to privacy. So many times I hear from privacy officers who I think are operating under principles that we’ve been through in the 1970s and the 1980s. My pet peeve is to hear, as I did on a blog devoted for privacy professionals just this week, privacy is so hard to define because it means different things to everyone. As somebody who spends his career in this area I don’t believe that, and I’d like to try to update you on what I think is the current trend in the privacy field.

There’s so many misconceptions that privacy means you can’t even give the information to the individual himself or herself, or that it says you can’t store personal information. A lot of people think privacy and security are synonymous. They are not. A lot of people think privacy protects organizations, and it does not. A better term for that is secrecy or confidentiality.

So I’m going to take as an example the NSA surveillance as revealed by the Snowden disclosures, not to discuss that, but to show it as illustrative of what I think is the current trend.

Back in 1979, the Supreme Court said that numbers dialed to and from a phone are not entitled to privacy protection. They’re not as sensitive as the content of the conversation. Back then there was a device called a Pen register which you could hook up to a phone, and it would record, for law enforcement, the numbers dialed in and the numbers dialed out. And the Supreme Court said that law enforcement does
not need prior approval for this because it’s not as sensitive as the content, which just about everybody knows, since the early 1970s, you have needed court approval to record the content.

Well, in 2014, the opposite is really true. Most cell conversations are not that probative. They’re not that sensitive. Think about your own calls. I’ll bet most of them are to make appointments, and to change appointments, and to meet people at certain places, and I wonder just how sensitive is the information in your average cell phone. But the numbers that you dial to and from that phone are extremely probative. They really show who our associates are and our patterns. And NSA has said as much, that that’s precisely why they want to gather that information. It’s called metadata, and now, finally, probably you know what that term means that we’ve read in the paper for the last six months. Metadata is no more than the numbers dialed to and from a call and also the nearest cell tower that might handle a call. And an example that’s often used is that when you call an abortion or AIDS clinic, you’re most likely not even going to mention the name of that clinic or the ailment that you’re calling about, it’s going to be to make an appointment. But it’s the number called and the fact that you have an appointment at a certain time that is extremely revealing and tells about the associations of people. So, NSA, as I say, has recognized that.

So now look in 2013, just before Christmas, the court decision that you probably read about. It’s important to realize this one came out of the Southern District of New York. The main thrust of the government’s argument here is that under Smith, that’s the decision we just talked about in the previous slide, no one has an expectation of privacy, let alone a reasonable one, in the metadata that telecom companies hold as business records. And then the Court said, boldly, When do the evolutions in the government’s capabilities, citizens’ phone habits, and the relationship between NSA and the telecom companies become so thoroughly unlike those considered by the Supreme Court 34 years ago that the precedent in that decision simply does not apply? The answer is now. and why is that?

Let’s take a moment, though, for a poll that this technology allows us to do. I’d like to know, which is the most sensitive in your environment and provide us an answer please.

So, Robert, this is a particularly apropos topic for what’s going on and it’s good with privacy. I’m intrigued about the metadata because I’m actually involved in some projects where we’re using metadata to help us track disease and illness and some of those other things. And so there are really good reasons why that data can be used. How do you separate the good from the nefarious?

Well I’ve always thought that the protocol that we’ve had in place for many, many years is the appropriate one, that we need a data trail whenever law enforcement or any administration wants access to that information. A court can give permission for that, and then whoever might be victimized later on at least has a paper trail that you can go back and check. But I certainly recognize, I think we all do, the need for law enforcement to have that information. But the methodology of getting that information is what is at issue. And I think court approval is the appropriate protocol. These laws all have emergency contingencies if that’s necessary. It is possible for law enforcement to get the content of conversations and then go back and get the approval of the court afterwards.

All right. Looks like the poll is pretty much finished. You might want to grab that and keep on.

Yeah, I’m interested that the location of a person in real time is not regarded as the most sensitive. We’ll see later whether, in fact, universities do collect that kind of information. I think inadvertently they may.

Mark, how can I – oh, you just answered my question.

So, another point that the Court pointed out, that cell phones are no longer just telephones. They really aren’t. they’re little computers that we carry around. They’re little GPS devices that we carry around. So they’re now multipurpose devices. They have maps and music players. That’s another reason why this metadata, so called, is much more sensitive, really, than the content of our conversations.
Educause

Educause Live_Location, Location, Location

I’m going to switch the subject a little bit, and let’s poll about security breach notification. I assume everybody knows what that is. Are you aware of what the requirement is in your state?

So, Robert, that’s actually kind of interesting, because as I changed states, the – is there a commonality to the law, a baseline, and maybe after the poll you can help us. I’m always confused at the different requirements of reporting and mandatory requirements if it’s a financial breach to put them on monitoring and all those other types of things.

It’s been interesting to me that business has tolerated such inconsistency because normally it says we want uniformity. That’s why they go to Congress, we can’t comply with all these different state laws. The state laws are quite different. You know, their basic requirement is that you have to notify the persons potentially adversely affected whenever there is a breach in your organization. And they apply equally to higher education, and medical institutions, and others. But they all differ quite a bit. One state, Pennsylvania, requires notice to the news media. I would say about a quarter of the states require notification to the Attorney General of the state. Some states that certain personal information that’s breached triggers the requirement, others define personal information quite loosely. There seems to be inconsistency as to what is timely notification. Some states say 48 hours. Others give a little more leeway. So all but, I think, four states now have these requirements, and it’s really important that you know your state requirement. And as you say, when you change jobs and go across state lines, you’re going to have to learn all over again because currently the security breach notification laws are slightly different in every single state.

And a good time to turn you back to the poll because I’m, frankly, a little surprised that a big portion of our audience is not familiar.

Yeah, that makes you really vulnerable because if there’s a breach today as we speak in your organization, some states are saying that within 48 hours you better notify those people who are affected. And you’ve got to know who’s adversely affected. And a lot of those people who are affected might be out of state, so that’s another consideration.

But let’s have another poll. What is the federal breach notification requirement?

Now this one you’ve got me stumped, and I’m anxious to see what the audience says because I’m very familiar with my personal state and kind of interested in what we get back from that. There’s a huge –

No clue. I like that answer.

Yeah.

But it’s close to the right answer. Just about everybody’s got the right answer. There isn’t one, with two exceptions. The HIPPA law, which requires confidentiality in medical information, does, in fact, require breach notification, and, indeed, notification to the federal Department of Health and Human Services, which is required by law to post those breaches on its website. So if you have a medical institution within your organization, be aware of that, that there is that federal requirement. There’s also one for financial institutions, but most of the people in this audience don’t have to worry about that. So just about everybody had the right answer there. It’s mainly a state requirement.

So I’m going to call Glenn Greenwald here. He’s a reporter for The Guardian, who broke the stories with regard to the Snowden disclosures. And we’re not going to argue pro or con whether he’s a good guy or a bad guy or whether the disclosures were right, but I think in testimony before the European parliament just before Christmas he put his finger on the very same trend that the judge in New York said.

If you talk to surveillance experts, what you will hear around the world is the collection of metadata, which we’ve already talked about, is not as invasive as the interception of the content of conversations. But collection of metadata is now more invasive than the intercept of content. That’s the message.
I want to also point out, I know many of you know that a federal district court in Washington came out the opposite way just before Christmas and said that the NSA disclosures were not illegal and not unconstitutional. So we’re not going to debate the merits of that and I’m not getting into that case. I only want to use the case in New York because it’s illustrative of this new trend that Greenwald also put his finger on. In fact, Snowden told Greenwald that the main reason he was motivated to make his disclosures was that NSA was now in the business of collecting information about the numbers dialed to and from a phone.

So Greenwald said it’s difficult to understand that in the abstract, but it’s easy to understand when you have concrete examples. That would include, as he says, when a woman calls an abortion clinic, or a patient calls an AIDS clinic, it’s going to be the phone number that probably gives away most of that personal information more than the content of what’s said over the telephone.

I’m happy to take any questions that you might have as we go along, and Mark will handle those. Let’s do another poll, though. And we’re back to breaches of data security. And remember, we’re talking only about breaches that involve personal information, information about people. If you’ve had a breach involving financial information in the university’s system, we’re not talking about that today. Privacy involves only information about people.

So, Robert, in your previous slide you talked about the information about where you call that could be just as vital. There’s a story that runs around about privacy of information about – and I believe it’s not just a story – about some store that kept track of people and when the spouse was looking for pregnancy tests ended up sending an email about discount on diapers and therefore breached the privacy and exposed that the wife was potentially pregnant. And that’s a great example of metadata and how it is used poorly. Are there rules on that type of thing for stores and credit card companies and those types of things?

Well, the Federal Trade Commission imposes privacy requirements on businesses, which essentially says that once you post the privacy policy, you better abide by it. So if you’re going to tell folks that you respect their privacy and list how you do it, if you breach that yourself, if you don’t comply with your own privacy policy, the Federal Trade Commission will regard that as an unfair retail practice. That would not apply to higher education. We all know that there are (inaudible) regulations with regard to the disclosure of student information. But it’s important to recognize that more and more now the disclosure of that information may not involve academic records, but may involve other things like consumer choices, as you pointed out.

So here we have the numbers of people who have had to report a breach. I’m surprised more people didn’t want to vote because I’m not sure you’d want to disclose if you have had that breach, but I presume it was reported properly. Let’s move on.

Here, once again, is Greenwald. It talks about if you are collecting this information you will see the phone number that this person called, etc.

But there’s another factor here that Greenwald points out. Not only is this information what a lawyer would callprobative, that it tells something about people, but the ability to analyze it is much, much more sophisticated. Back in the days of the 1970s when we had this device that now seems primitive that merely attached to a telephone and collected the numbers called to and from. So NSA is gathering information about numbers called to and from on a massive basis. But it also has a sophisticated analysis to analyze that data. If you did this individually, just imagine how labor intensive this is. But NSA does have the ability to analyze this by key associations. Whenever they see a repeated phone call to a certain person that is a target of their interest, then that’s going to make them perk up and they’re going to be interested in that pattern. So this can be collected now en masse, in huge numbers, and can be analyzed to find out people’s patterns of who their associates are, and also, because it does collect cell phone data, it also tells about their travels around town. And he concludes by saying you have a very invasive understanding of the private behavior, the private associations, the private thoughts of people whom you place under surveillance.
Now we can debate whether this has great relevance in the higher education community, but I think it’s very important for everybody to realize that this is the new trend, I believe, in privacy, that it’s the location of individuals as well as the phone numbers that they’re calling and those numbers calling to them that is much more invasive, actually, than the content of their messages. And that’s what this slide tells us. Data about our calling patterns is far more sensitive than the content of our calls.

So how do we deal with this? I think first we look to the traditional principles that have guided privacy protection over the years. I hope that people are familiar with these, the Fair Information Practices. The Code of Fair Information Practice developed back in the 1970s by a very notable study done by the U.S. Department of Health, Education and Welfare, then called HEW, now called HHS. This was not a reaction to Watergate, but a reaction to increased information collection by huge computers and huge organizations. This was before the internet, before email, and before hand-held devices.

Let’s see whether that code does apply in the era of the collection of metadata and location data.

The first principle is that the existence of any data system ought to be publicly disclosed. And I hope every university does follow this. And people have to know the purpose for which the information is gathered, and we’ll see in a minute why this is really crucial. And call this one the principle of openness or transparency.

Next there must be a way for an individual to find out what information about him or her is in a record and how it is used. I mentioned earlier that privacy and security are not synonymous. Here they conflict. You’re asked to build a system that is secure against all outsiders, yet you’re asked to build a system that can accommodate an individual who wants to know what information you have on him or her. You have to deal and reconcile with that conflict.

Next, there must be a way for an individual to prevent information about him or her that was obtained for one purpose, which was stated when the information was gathered, from being used or made available either within the organization or outside for a purpose that is incompatible. Now this is the most important principle. It’s the one least known, and the one most violated. It’s the principle of secondary use. We talked earlier that an organization should not only disclose what kind of information they gather, but why they want it, what’s their purpose. And here’s the reason for that. It ought to stick to that purpose. If you gather information about a student’s address to find out where to send a report card, you ought not to use that for marketing information. That’s a secondary purpose, and that’s when institutions get into trouble.

Another point here is that information may be disclosed even within an organization and be an invasion of privacy if, in fact, you’re disclosing that information for an incompatible purpose. If you were to take information from your data system and to provide it to a professor, let’s say about the grades the student is receiving, and the professor has told you it’s going to be used for a non-academic use like to organize a social affair, that’s an incompatible purpose, and whoever the data administrator is ought to be aware that that violates this principle, this principle of secondary use. Anybody have any questions about how that operates?

I’ve been writing a whole list for you, Robert, and kind of interesting because of all the things that we’re doing. And I think, if it’s okay, I’ll start with the FERPA data. You know, all of us collect stuff on students’ grades, their participation in class. Sometimes we take attendance and how much they’re on the web and interacting with the online courses. And we collect that both for giving grades and giving exams, but then we also try to use that to protect the student, look for their success, look for where they’re doing poorly, try to advise them on that. Is that a secondary use that’s not acceptable?

Depends on how you define secondary use originally. If you want to define it broadly, that we collect this information as part of our academic mission, that’s a very broad purpose but it will cover you. On the other hand, individuals may be reluctant to provide information because it’s too broad. So the institution itself articulates what the purpose is. If it’s a broad one, then you’re covered. If it’s a very narrow one, you will win over their constituency but you may limit yourself later on.
What about employee data, because, you know, we have similar types of data on employees, and, you know, yes, I don’t want that data — you don’t want a supervisor to be able to go in there and look and perhaps see what an employee’s doing, but the same easy set of rules? Just tell everybody what you’re doing and you’re okay?

Well, not quite, but there is no law that governs employee records as it does student records and medical information, so that’s the first thing to remember. But I believe all organizations should comply with this code, and that would mean any employee information, you would tell the employee what kind of data systems you have and why do you collect that particular information. That, by the way, reassures a lot of people. Once you tell them why you need the information, they’re much more comfortable about providing information. It also helps you with your disposal policy, too. I wonder how many people know that many states have rules now about when you have to dispose of data. So if you’ve articulated the purpose of the information carefully, you’ll know when to dispose of it because that purpose has become obsolete. So that’s another reason that it’s an important thing to do.

Somebody has asked whether higher education institutions should post a privacy policy. I would say absolutely. You’re going to find little crevices of the law and regulations that require it. So be safe and have one. It’ll also help you very much in being able to explain to those not in the IT field why certain precautions are necessary. For instance, I wonder how many people listening know that if you’re gathering information about Massachusetts students, you’re supposed to have a security policy. On file. That is a requirement of a rule of Massachusetts that the courts have said is appropriate even though it reaches beyond state lines.

I do business in Rhode Island. I have a security policy for my small organization because I gather, however small, information about Massachusetts residents. So keep that one in mind.

So I’ve got another one for you as we dig a little deeper, because it gets fairly complex. So we keep network data in order to keep the network flowing correctly. Right, what’s happening, where’s the bottlenecks, you know, how do we shift and adjust the load so that we can keep the data flowing smoothly, all those types of things. That metadata could be used for other purposes. Now, from what you said, if you’re using that on a student, that’s considered FERPA protected I assume.

Yes, well, to the extent that it’s a student record, yes.

And so if we wanted to use that data in order to see how active students were in order to find out if they’re spending too much time on the internet and not doing their studying, acceptable?

You’d be perfectly acceptable if the data is not personally identifiable. This code, and most of the laws, are triggered when we’re talking about personally identifiable information. So the extent that it’s cumulative, that it’s anonymous, the theory is that’s not going to hurt anybody, so you can analyze it as you wish if it’s cumulative and anonymized. So do that first, and just to be careful, encrypt it. And I have a rule of thumb that’s not part of this code, but I don’t think that any information that identifies individuals should be on portable media. I am not in the higher education field, but I believe that organizations ought to find a way to run their data systems without carrying around personally identifiable data in portable media.

So there’s a question over here that kind of digs deeper. So a meal card, gym usage, participation in different clubs, every time they enter and exit their dorm, their housing unit. If that’s helpful, if we determine in an aggregate that that’s helpful in determining a student’s success and then want to go to identify students that fit the patterns that tend to cause those students to fail, is that part of our mission?

As the institution articulates it, and I think that, you know, as a lay person, I find that a valid mission. I think that as long as the information is cumulative you don’t have a privacy problem. Once you identify people, then you would go back to your privacy policy, look at these principles, and make sure that you’re complying with these principles as you go along. Have you announced this data system? Have you told
people what it gathers? And look at this new principle that I posted here. Do individuals have a way to correct or amend that information? If it's individually identifiable, I think it's quite conceivable that at some point it could affect a student or employee's welfare at the organization. So that's why you need this right of correction. And if you have provided that, you're going to lessen complaints, believe me, from students and from compliance officers.

And is firewalling that data sufficient, meaning we collect all that data, and we may anonymize it and use it for bigger trends but then require special permission to go in, such as an advisor who's trying to find out if a student is doing okay would have to get special permission to go in and look at the individual student. Is that sufficient?

I can't articulate whether that is sufficient, not being a technical person, and I think that complies with the spirit of this code. Whether it complies with the actual letter of the law, who knows. I don't know, put it that way.

Okay.

But you have reminded me of an important thing about these security breach notification laws, these state laws that we talked about earlier. Many states say if the data is encrypted, you're free, you're not covered by this law. So that's an important thing to know.

Encrypted meaning it doesn't get breached? Or, actually, if it is breached but all they get is an encrypted copy, then you're not held accountable?

No harm, no foul, as they say in North Carolina.

So there's lots of people, and I'm not sure you're going to be able to give details, but they're like -- and it's a big one for fundraising. You know, we have the students, they're alumni, they're parents, we have all that information, and the fundraising activities would love to have that information in order to be able to use it. As long as you warn people you're doing it, that's okay? Seems to be what you're --

Yes. I want to stress that FERPA applies to student records, not parents' records like this. And I do recognize that a lot of the universities do this. But I think technically as a matter of good practice, you should look at this code, and comply with it, and tell parents when you're gathering that information what's the purpose for it and why you need it, and indicate when you would disclose it. That means that some people will not cooperate and provide the information, but it will also mean that if you're caught, you won't be in trouble because you've already articulated the purpose for the information.

And my understanding of FERPA is that if we're using it for the educational betterment, for the activities and the business of the university, that we can use FERPA data internally, but this is a separate instance that you're talking about that has to do with the rights of people knowing how you're using their data as opposed to the law saying we can't use it.

Well, I was just differentiating between students and non-students. There are no regulations, federal or otherwise, with regard to non-students unless there is a breach of fundraising data, then you would have to notify those potential victims, yes.

But on the flip side, if I wanted to use all of the student data, legally the institution is allowed to use that data at the current time. Am I misunderstanding?

I think you'll have to go back to the FERPA regulations and make sure you're on good grounds there because you had said that you disclosed this data within the university to further the university's mission. That sounds extremely broad to me, so you would certainly have to use academic information for an academic purpose.
Right. Okay. And as long as you had a form that when the student submits their application and accepts their attendance – and that’s going to relate to my other question – if they consent to this, then all problems are solved. Is that true?

If the consent is knowing, yes. And you’ll find that universities are doing that now with the registration of the students. It’s required by FERPA that you not only articulate some of these purposes, but many people may know that certain directory information about athletes’ performances and about what grade a person is in and all that, the address of a student, phone number, that can be released unless the student speaks up and says I don’t want it released. So all of that is usually done in September at registration time.

Okay. And I’m going to go a little bit outside of higher ed for a second because it relates, and we all use the click wraps. You know, you go to Apple and you want to use iTunes, but more importantly you go to Google and you’re going to use Gmail in the business setting, and all those different things, and their terms, everybody clicks on and says sure, yeah, doesn’t even bother to read it. And they collect more information than a lot of cases NSA is. Is there, by consent, the fact that we’re clicking that button then everything is okay or is that a misconception?

I’m not sure I agree with it, but in my home state a court has ruled that if you click through, you’re consenting. Everybody knows, and the court said this, everybody knows we don’t read that stuff, but if you click, yes, you are bound by that consent, so you are covered. Whether that will last, I don’t know, but currently that seems to be the law that people who unknowingly, who without thinking, simply click through that, are consenting to everything that is in that small print.

So there’s a question down at the bottom – and I want to make sure you have enough time to finish your slides. I think we’re –

I’m in pretty good shape. Yeah, thank you. I’m doing fine.

Okay. So there’s a question at the bottom that says okay, so we’re doing a lot of outsourcing. Cloud services, contracting for services, how do you represent that in the contract, that the contractor is held to the same standard we want to hold our institution to?

Indeed contractors are held to the same standard, and you’ll find plenty of language on the internet because other organizations have dealt with it, where you simply pass on the privacy obligation to the contractor. Contractors have certain obligations with regard to security breaches as well. So that’s something you’d want to notify your contractors of, but I don’t think you’ll have a difficulty on the internet finding sample language for those contracts.

And so essentially saying here’s our privacy policy, we expect you to enforce it with our contract is a practical way to go in some manner.

Precisely. You may want to even say more, whether there’s a legal obligation to do that. In some cases there is, so I think you should put it in the contract that you have taken on these privacy obligations pursuant to such-and-such a law. If there is no law, then it is simply a contractual term between the university and the contractor.

All right. I’m going to let you get back to a few slides rather than continuing to pepper you with questions and I’ll write some more up.

Well I’ve got time for a couple more because I am ahead of schedule.

Okay. Well then there’s another question that says okay, they like the Code of Fair Information Practice and are comfortable with that, but it’s not really easy to enforce in that there are no real laws behind it right now, I think is what the intent of the question is. And the question really is, do you see any
movement in a comprehensive privacy framework such as the EU has and that the U.S. might come up with a statement that kind of makes a global statement on privacy?

That's a good observation. This code is part of the federal Privacy Act which applies to federal agencies. I think you can say it’s part of FERPA, which applies to educational institutions that get federal money. It’s really incorporated into HIPPA, which is the federal medical confidentiality rule. There are some other laws that incorporate this code, so it has gotten a very good reception. When it was first devised, there was a huge debate as to whether it should apply to the private sector. It’s not a relevant argument in higher education because, as we know, higher education is covered by a law that was passed the same year as the federal Privacy Act. But let’s take your local mom-and-pop store or General Motors. No, there is no such obligation. There have been attempts to do it. We choose in the United States to apply privacy principles to individual sectors, whether it’s higher education, medical records, credit records, financial institutions. We don’t cover everybody. That’s called the omnibus approach, and that’s been the European approach, and the debate wages as to which is the better way to do it. In Europe you can be assured that any organization you deal with has to abide by this code. On the other hand, the code applies to a lot of records we could care less about, and you’re going to get an awful lot of paperwork at your home telling you about consent and waivers and all the like about information you really don’t care about. So I think I favor the American approach, even though it happened accidentally, that we cover only those records that are most sensitive. It’s more complicated for the consumer I concede, but it doesn’t cover a lot of records that we really don’t care about. I think we’ve all seen the paperwork that was generated by the financial privacy regulations about a decade ago, and we all know the paperwork that’s generated by FERPA. So I like the sectoral approach. The Europeans choose the omnibus approach. Canadians, naturally, as Canadians do, have picked part of the European approach and part of the American approach, but he questioner puts his or her finger on a very good observation that this entire code applies to everybody in Europe, including mom-and-pop operations. In the United States, we apply it only to those very sensitive records.

So that’s – I get that, and I can see how that reduces the workload, but your example on the telephone records is a good one that says we didn’t think that record was important until now you start getting the collective vision of it and the ability to do analytics and all of a sudden it becomes important.

Indeed. And I think the one thrust of my presentation is that we have to question whether this code does cover what’s called metadata. In many ways it doesn’t, you know. Is the right of access, the right to correct or amend, really meaningful in such a massive collection. And we may well have to add to the code or tighten it up in this way because no phone company ever disclosed to a customer that this information might find its way to a government intelligence agency which will not only collect it about every single person involved, but has very sophisticated tools, digital tools, for analyzing it. So I’m questioning, indeed, and that’s one of the themes of my presentation, is this code adequate to cover that, and that, I think, echoes what I began the session by saying, that we can’t enforce privacy principles with 1980s knowledge of what is involved. The framework, I think, has changed in 2013, and that’s the message here.

Let me just –

Please.

Go on with kind of a summary, which I skipped. Anyway, let me read it to you. I’m talking about the importance of location now as a new data factor that probably is more sensitive in the privacy world than some of the others.

Think about all the times in your life just today where your whereabouts, in real time, is recorded. Using an ATM machine, the location where you were is going to be known in real time and will be archived. Your GPS in your automobile or in your mobile device. The cell phone tower that’s nearest to the phone call that your’ dialing or will dial after you finish up here today. Think of the cameras in every one of your communities on street corners and in shopping malls and in office buildings and parking lots, all over the campus. All of that archived and could presumably be analyzed, once again, by sophisticated computers
to find out whether a certain individual with a certain face, based on face recognition, was in a certain place at a certain time. So all of those things now contribute to a reality that the location of where we are is a part of databanks as much as what our medical history is or what our credit history is. And think of somebody – you mentioned it earlier - the ID cards that are used on a campus, to either get a meal, or to get access to a dormitory room. That tells a person’s whereabouts and the time that they were there.

And think about Street View. I realize that’s a stagnant, still photograph of a location and so it won’t show in real time who’s walking by my house or your office, but it is a collection of photographs of every single bit of real estate in the United States, and, indeed, overseas. And Google isn’t satisfied with that. It’s moving on to collecting photographs of the interior of buildings. It may well have done that on some of your campuses. I’m not sure how it resolves the access issues, but I do know that its current goal now is to have Street View available within large interior spaces that are used by the public.

I’ll take some questions in a minute, but let me give you some resources now to – unabashedly, the first one is published by us. Every year we do a compilation of state and federal laws including all the security breach laws and the differences and the nuances. We just recently updated. It’s available in hard copy or in electronic copy.

And next I published back in 2004 a book about privacy in American history. And I think it’s important to trace how we got some of these requirements and not think that they just suddenly emerged in this current century. The concern about Social Security numbers stems back to the 1930s, for instance, and concern about eavesdropping came about just after the Civil War with the introduction of the telephone. And the so-called torts of invasion of privacy. Not something that comes up in the IT community very much, but you can bet that the general counsel’s office at universities have to worry about that, and that’s the sort of garden variety of invasion into people’s space, or disclosure by a newspaper or somebody else about private information about them. Those kind of wrongs are still alive and well. And I try to trace how they developed and how they have relevance to a compliance officer in this current decade.

I’m really proud of this study in 1997. A little bit dated, but I was on that task force and had a very good experience hammering out the requirements in the higher education community trying to tell people how to adapt the FERPA regulations to the networked environment.

And we just published in the latest edition of the newsletter, which I’ll be happy to send to anybody, electronically or a hard copy, who wishes it, describing some of these nuances among the state laws. Probably nobody in the audience does business in two states, but it’s possible that some do, and so you might have different requirements in different states, and abutting states as well.

And don’t forget that, and I’m not sure how this is worked out in compliance terms, but you all have out-of-state students. If you have a breach, I think you have to differentiate between those students who live in State A with one requirement and those who live in State B who have a different requirement. There’s different notice requirements. It affects not the site of the university, but the residence of the students.

And next an interesting article that you might mention. This is a little bit off topic, but some of you may be interested in whether admission offices, and, indeed, employment offices, are using Facebook and Google. Indeed they do, but I don’t think it’s as overwhelming as we first were led to believe. But at any rate that was an interesting account by how much that is being done. Students seem not to be worried about this at all. Maybe they know something we don’t know. And then the Kaplan test prep did a survey about use of Google by admissions officers and students’ reaction to that.

Our newsletter is called Privacy Journal, and I’d be happy to send a sample copy to anybody. If anybody has questions afterward, send an email to that address and I’ll try to help you out.

And I’m ready for questions.
Great. So the one that – let me get a couple that were asked and then I have a bigger question. So one of the questions was about Cloud services, and we actually had to face this. So you want to use Drop Box, you want to use Google, you want to use anything you want. Anybody can go in there and click through the terms, start using it, and not follow the privacy and security and retention policy if they choose. And in large distributing campuses that's pretty hard. Do you have any advice on how you, you know, if we have this great statement, how you get people to follow it and enforce it?

We're getting towards the end of the hour. We're rapidly getting passed my technical expertise. All I do know is that the Cloud information is still within the custody of the university, and it is covered by these regulations. So that doesn't obviate these responsibilities even if there's no state line that applies because it's in the Cloud. But that information is still under your custody so that you have to get your contractor to agree to comply either with your legal requirements or with the requirements of your voluntary privacy policy. And I would think in a university environment you have both.

Yeah, we do. And my biggest concern, and I’m sure for many on the phone line, we have things that have been sitting around since the beginning of the internet. We had a – a different location that I was at had a – one of the reasons (inaudible) your poll you had a serious breach, and the word serious scared me. I didn’t answer the poll, but I’ve had what I would consider much more minor breaches, but nonetheless we had to take care of them. And some of this information has been sitting around for five and ten years on some faculty member’s website that just has never been erased, never been changed, and was before some of these laws had strict requirements. And so it’s the leakage of data that concerns us more often than the willfully breaking the rules. And yet we’re still liable.

Yeah, that’s right. First that reminds me that there’s been a lot of complaining about privacy requirements, but I think they have forced organizations to clean up their data and get rid of that which is obsolete or which is not necessary. First of all, if you have to notify people what data systems you have, people in the university with responsibilities can find that out. And secondly you will find out what’s obsolete and no longer necessary. But also another quirk or consideration of these security breach notification laws is each state seems to define the seriousness of a breach quite differently. Mostly it’s defined by the number of people involved, or potentially involved. Sometimes that’s not easy to articulate. And it is also possible, I believe, that an organization could say we believe no one is potentially a victim here. And if you’re willing to stick with that, I believe that might relieve you of the notification requirement.

It’s important to remember, too, that each state law defines personal information in a breach quite differently. Nobody covers photographs for instance. That could be the greatest breach of all if somebody got into a photo system, imagine a breach into the Transportation Security Administration’s photo file at an airport. How sensitive would that be? Yet I know of no security breach law that covers that. So it covers, in many cases, just kind of identity information like account numbers. These laws were passed as a kind of a reaction to identity theft problems, not to more overall privacy problems, and so they define personal data not according to its sensitivity but more in relationship to how could it be used to co-opt your credit.

There was a question about an example of a serious breach. I think you kind of talked around that a little bit here, and it might be difficult to give an example. Do you know of any higher ed examples specifically that you would use to define a serious breach?

Yeah, I mean there have been several. I could suggest people go to a website, a privacy clearinghouse in San Diego, California, keeps a list chronologically of all the breaches. Many, many of them have involved institutions of higher education. I would say many of the two-year, level two, junior colleges, community colleges. They usually involved a corrupt employee on the inside or an unhappy student who happened to work in that office. But I noticed, especially in the early days of identity theft, that many of the incidents involving stealing of personal information did, in fact, involve universities and colleges.

So the struggle that I have with all of this is the balance between security and privacy. If you look at the London subway bombing, it was because they had all those cameras they were able to find the guilty
Well, security is one component of the Code of Fair Information Practices. We kind of skipped over it, but one of the components of the Code is that the custodian of the data has an obligation of security. Back in the 1980s that was not the case, and many organizations tried to shirk their responsibility.

It’s tricky. Sometimes they conflict, as I mentioned. Try to build a data system that gives individuals rights of correction and access and one that’s secure against the outside world. Not easy to do, but I think it has to be done. They can be reconciled, I do believe, by creative system design.

I want to go back to the previous question because it may have – I see on the screen here, can I give an example of a serious breach. I gave a hypothetical one involving all the nude images held by airport officials, but just the ones at Target and Neiman Marcus before Christmas are enough for me. Now they’re serious in that they inconvenience a lot of folks because those perpetrators, most likely overseas, will take that credit card information, those PIN numbers, and will charge products at other places. Now I think most people know that your liability is only $50.00, and you can tear up your credit card today and you can get a new number. So is it serious in that respect? Probably not, but information about adoption, about children’s whereabouts, children’s addresses, children’s images, about medical conditions that could cost us discrimination at work and could cost us a promotion, those I regard as very serious breaches, and they have occurred. So on the one hand breaches involving Social Security numbers and credit cards affect the most people, we hear the most about them, they cause the most inconvenience, they are the most value to the perpetrators, but that’s information that you can change. You can’t change your cancer diagnosis. You can’t change, easily, the address of your children. You can’t change your image so easily. So I regard the most serious breaches are those involving information about us that we can’t change.

So, Robert, we’re in the age of Facebook, social media, everybody has their own website, and we tend to share a lot of information about ourselves, and I know that’s not – I mean, if we make the decision to share it, then we’ve done that and we’ve consented to do that, but how do you get people to understand the implications of those sharing and the people like the Facebooks and Googles and Apples of the world who have all that data to understand their responsibility for having that data?

It’s the bane of my existence. I wish I knew the answer to that, but throughout my career I’ve been trying to get people to take this more seriously and to anticipate that their lives may change very quickly in unanticipated ways making certain information about them that they freely disclosed in the past, that information suddenly takes on great importance. I can’t tell you how many people come up to me and say they could care less about insurance information and who has it and whether their employer has it, personnel office, and they say but you know, now I have a chronically ill child and it means all the difference in the world to me, now I get it why my motto has to be, when in doubt, don’t give it out. I know that the information community says when in doubt, collect it. My word to them is when in doubt, don’t give it out. And you can’t anticipate when your life might change in that regard. So I’ve been trying to educate people about this, and now along comes a generation that lets it all hang out. That now will put anything on Facebook including their beer bashes, their embarrassing photographs, their stupid quotes, everything is up there, and they seem not to care. And Facebook is quite happy to make a buck off of all of this.

I think it’s going to crumble at some point. I think that young people are going to realize that that is not in their best interests. And more importantly, a lot of users of Facebook are going to start to say, well, why do I want to be exposed to all of this stuff? Do I really care about this trivial aspect of my friend’s life? So we’ll see how that goes. But people are much too willing to sacrifice privacy for just a little convenience. And I must say I don’t think I’ve succeeded in trying to point out to them the importance of this. And the importance of practicing. When I go to a point of sale and people ask for my zip code, that’s really harmless, but I practice. I just say no. So I get used to denying requests for personal information unless somebody can articulate for me why they need it. So, yes, the demand for a zip code is not going to cause you huge difficulty, but get in the practice of saying no. And also make sure that the word gets to
the people who manage that organization that people do care. That they better think twice before they ask for personal information that really isn’t necessary for the transaction.

Well, I’m going to give you one last short one. What do we do about the youth, because you mentioned them. I know that probably when both of us were younger you could do things and the permanent record didn’t exist because your friends knew about it, maybe some family or the neighbors, but it didn’t get broadcast, saved, stored and archived and searchable. Are people seriously talking about ways to protect youth from their indiscretions as they move on?

No, except I see some good stuff written in Canada, actually, about that, but I don’t think we understand our own kids’ use of Facebook. And the more we understand it, the more we can counsel them on that because kids do care about privacy. They care about it within the home. They do care if their parents are getting access to Facebook. So we just have to know more about their happens and find their point of vulnerability about privacy because in many, many ways teenagers care more about personal privacy than adults do. Of course they haven’t entered the credit/employment nexus yet, so they’re not too worried about that.

Judith had mentioned that after this seminar she now knows why she doesn’t use online banking. I hope to dissuade her from that. I use it. But what I did was practice. Somebody had told me that my Social Security number went out with my checks and all that, so I practiced. And I came to the satisfaction that online banking is safe.

So, Robert, we’re at the close of the hour. As you can see by all the chats, people really appreciated it. There were a lot of aha moments I think in people who started to understand the seriousness and the depth of all the information, what to do with it, so I thank you for both the audience and myself for your presentation. I want to thank all the participants online, and hopefully before you click off online you’ll notice there’s a survey we’d like you to take – it’s right up there on the screen – if you would, for how much you liked the webinar today, as well as the archived link so that you can go find the archive and share with the rest of your community what happened today and the slides. If you missed out on today’s conversation, don’t forget that archive.

Those of you online, Wednesday, February 19th at 1:00 p.m. will be our next Educause Live, The Geographies of Learning, How Students Navigate, Use and Learn With Digital Resources.

And with that, this has been a production of Educause Live from the Higher Education Technology Association. On behalf of Educause, I’m Mark Hoyt, and I want to thank you for joining us and we’ll see you next time. Robert, thanks again.